INSTITUTO DE ESTUDOS SUPERIORES MILITARES

CURSO DE ESTADO-MAIOR CONJUNTO

2011/2012

TRABALHO DE INVESTIGAÇÃO INDIVIDUAL

TERRORISMO: A INTERRUPÇÃO DE SISTEMAS

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IESM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS E DA GUARDA NACIONAL REPUBLICANA

ALEXANDRE MANUEL RIBEIRO DUARTE VARINO
MAJOR DE INFANTARIA

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

TERRORISMO: A INTERRUPÇÃO DE SISTEMAS

Alexandre Manuel Ribeiro Duarte Varino

Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto 2011/2012

Lisboa – 2012

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

TERRORISMO: A INTERRUPÇÃO DE SISTEMAS

Alexandre Manuel Ribeiro Duarte Varino

Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto 2011/2012

Orientador: Maj Tm Gustavo Ferreira Gapo

Lisboa – 2012

Agradecimentos

As minhas primeiras palavras de agradecimento vão para o meu Orientador, o Major de Transmissões Gustavo Ferreira Gapo, pela permanente disponibilidade, interesse e acompanhamento que, tendo permitido a minha total liberdade intelectual, procurou sempre reorientar-me e indicar-me a direção a seguir.

Expresso também o meu agradecimento ao Tenente-Coronel de Transmissões Viegas Nunes, ao Professor Doutor Marques Guedes, ao Doutor Rogério Bravo, ao Coronel Tirocinado António Tavares, à Doutora Isabel Pais e ao Engenheiro Lino Santos pelas importantes partilhas dos seus conhecimentos e experiências, as quais se constituíram como mais-valias para a elaboração deste trabalho e se encontram vertidas no mesmo.

Não posso, também, deixar de expressar um agradecimento muito especial a todos os Camaradas e Amigos que contribuíram para a realização e revisão deste trabalho com os seus conhecimentos e conselhos perspicazes e de grande valor.

Por fim – e até porque em minha casa é normal deixarem o melhor para o fim – agradeço à minha esposa, ***Ana*** e ao ***Miguel***, por toda a compreensão, ajuda e amor que demonstraram não só ao longo da realização deste trabalho, mas ao longo de todo o Curso de Estado-Maior.

A todos um bem hajam e muito obrigado.

Índice

Resumo

O terrorismo é bastante antigo e tem acompanhando a evolução da humanidade, adaptando-se e, incorporando os fatores relevantes dessa evolução. Existem muitos conceitos de terrorismo, sendo no entanto possível identificar algumas caraterísticas comuns como a imprevisibilidade, a enorme e indiscriminada violência utilizada, os objetivos políticos, religiosos ou ideológicos e em que o alvo preferencial é a população.

A evolução dos sistemas de informação e de comando e controlo leva a que estes tenham nas sociedades modernas um papel central, ocupando a internet um lugar de destaque. Atualmente, todos os principais sistemas de um país são geridos, ou dependem de alguma forma, de sistemas informáticos, surgindo assim o ciberterrorismo como uma ameaça bem real que coloca em causa o seu normal funcionamento.

O presente trabalho, procura analisar qual o impacto que a interrupção dos sistemas de informação e de comando e controlo, provocada por ataques ciberterroristas, tem na vida das pessoas e nos Estados, identificando o que está a ser feito em alguns países de referência na prevenção e combate desta ameaça, e verificando qual a realidade nacional nesta área.

Desta forma, seguimos o percurso metodológico proposto por Quivy & Campenhoudt (2008), apoiados numa pesquisa bibliográfica e documental sobre o tema proposto, recorrendo essencialmente a documentos oficiais, a trabalhos e estudos publicados e ainda a artigos de revistas desta área do conhecimento, que complementámos com a realização de entrevistas e assistência de palestras, conferências e seminários.

Assim, este estudo vem demonstrar que a capacidade disruptiva dos ciberataques pode provocar não só elevados prejuízos e perdas económicas, como colocar em causa a segurança e o bem-estar nacional e internacional. O ciberterrorismo representa uma alteração estratégica na atuação dos grupos terroristas, tendendo a ganhar preponderância, o que eleva o ciberespaço a um novo campo de batalha. Os países, tendo consciência desta nova realidade e das suas capacidades, devem implementar medidas de proteção e desenvolver estruturas de prevenção e combate a esta ameaça.

Portugal tem algumas organizações que desenvolvem ações de proteção e combate aos ciberataques, mas não dispõe de uma entidade primariamente responsável pela coordenação de uma resposta concertada no domínio da cibersegurança. Para que o país possa vir a ter um sistema de segurança realmente eficaz, existem vários aspetos que necessitam de ser melhorados, entre os quais a criação de uma Estratégia Nacional e de um Centro Nacional de Cibersegurança.

Abstract

Terrorism is quite old and has accompanied human evolution, adapting itself and incorporating the relevant factors of this evolution. There are many concepts of terrorism, however, it is possible to identify common features such as the unpredictability, the massive and indiscriminate violence used, the political, religious or ideological objectives and also wherein the target is the population.

The evolution of information and command and control systems takes a central role in modern societies where the Internet occupies a prominent place. Currently, all major systems of countries are managed or depend, in certain ways, of the computer systems, emerging the cyber terrorism as a very real threat that puts into question its normal functioning.

The present study seeks to analyze the impact that the disruption of information and command and control systems, caused by cyber-terrorists attacks, has in people's lives and also in the States, identifying what is being done in some reference countries in the prevention and combat of this threat, and checking what is the national situation in this area.

This way, we follow the methodological approach proposed by Quivy & Campenhoudt (2008), supported by literature and document search on the proposed topic, using essentially the official documents, papers and published studies and also magazine articles of this area of knowledge, complemented by interviews, conferences and seminars.

Therefore, this study demonstrates that the ability of disruptive cyber-attacks can cause not only high damage and economic losses, but it can also question the safety of national and international well-being. Cyber terrorism represents a strategic change in the activity of terrorist groups, tending to gain dominance, bringing cyberspace to a new battlefield. Countries being aware of this new reality and its capabilities, should implement measures to develop and protect preventive structures to combat this threat.

Portugal has some organizations that develop combat and protection against cyber-attacks, but does not have an entity primarily responsible for coordinating a concerted cyber security response. In order to ensure a truly effective security system, there are several aspects that need to be improved, including the creation of a National Strategy and a National Cyber Security Center.

Palavras-chave

Ciberespaço, Ciberterrorismo, Infraestrutura crítica, Internet, Interrupção de sistemas, Sistemas, Sistemas de informação, Terrorismo.

Lista de abreviaturas, siglas e acrónimos

A	ANACOM	Autoridade Nacional de Comunicações
	ANPC	Autoridade Nacional de Proteção Civil
	ANSSI	*Agence Nationale de la Sécurité des Systèmes d'Information*
B	BSI	*Bundesamt für Sicherheit in der Informationstechnik*
C	CCD CoE	*Cooperative Cyber Defence Centre of Excellence*
	CDMA	*Cyber Defence Management Authority*
	CEMGFA	Chefe do Estado Maior General das Forças Armadas
	CERT	*Computer Emergency Response Team*
	CIA	*Central Intelligence Agency*
	CNC	Centro Nacional de Cibersegurança
	CNPCE	Conselho Nacional de Planeamento Civil de Emergência
	CSIRT	*Computer Security Incident Response Team*
	CSOC	*Cyber Security Operations Centre*
D	DHS	*Department of Homeland Security*
	DoS	*Denial-of-Service*
E	EM	Estados Membros
	ENC	Estratégia Nacional de Cibersegurança
	ENSI	Estratégia Nacional de Segurança da Informação
	ETA	*Euskadi Ta Askatasun*
	EUA	Estados Unidos da América
F	FCCN	Fundação para a Computação Cientifica Nacional
	FFAA	Forças Armadas
	FP 25	Forças Populares 25 de Abril
G	GNR	Guarda Nacional Republicana
	GNS	Gabinete Nacional de Segurança
H	H	Hipótese
I	IC	Infraestruturas críticas
	ICE	Infraestruturas críticas europeias
	ICN	Infraestruturas críticas nacionais
	IRA	*Irish Republican Army*
L	LOBOFA	Lei Orgânica de Bases da Organização das Forças Armadas
N	NATO	*North Atlantic Treaty Organization*

	NBQR	Nuclear, Biológico, químico, ou Radiológico
	NDPP	*NATO Defense Planning Process*
O	OCS	*Office of Cyber Security*
	OI	Organizações Internacionais
P	PEPIC	Programa Europeu de Proteção das Infraestruturas Críticas
	PIC	Proteção de Infraestruturas Críticas
	PJ	Polícia Judiciária
	PNPIC	Programa Nacional de Proteção de Infraestruturas Críticas
	PSP	Polícia de Segurança Pública
Q	QC	Questão Central
	QD	Questão Derivada
R	RAIC	Rede de Alerta para as Infraestruturas Críticas da União Europeia
S	SCADA	*Supervisory Command and Data Acquisition*
	SCEE	Sistema de Certificação Eletrónica do Estado
	SEF	Serviço de Estrangeiros e Fronteiras
	SIS	Serviço de Informações de Segurança
T	TIC	Tecnologias de Informação e Comunicação
U	UE	União Europeia

Introdução

O mundo de hoje é um mundo de mudança e grande velocidade. Pode caracterizar-se pela frenética competição em todos os domínios, pela contínua transformação e pela exponencial evolução tecnológica registada nas últimas décadas. É um mundo sem limites, quase sem fronteiras, em cadeia e ligado em rede. É o mundo da globalização, da informação e da tecnologia.

Da vida globalizada em que vivemos, fazem parte um conjunto de serviços essenciais e produtos, muitas vezes interligados e interdependentes. A interrupção desta cadeia origina uma sequência de acontecimentos, por vezes de dimensão imprevisível, influenciando negativamente o normal desenrolar da vida das populações. A prevenção e a contenção da interrupção deste tipo de sistemas, bem como a rápida e pronta resposta no sentido de os restabelecer, caso não tenha sido possível impedir a sua interrupção, são tarefas dos órgãos de soberania de qualquer Estado, das suas Forças de Segurança, de Proteção e Socorro e das suas Forças Armadas (FFAA).

As sociedades atuais são constituídas por redes mais ou menos complexas, tais como as redes de transportes, de comunicações, de abastecimento de bens, de energia, de distribuição de água, de telecomunicações, de atividades financeiras, económicas e comerciais, sendo que, cada vez mais, se depende destas redes e dos sistemas informáticos que as gerem e fazem funcionar.

Os sistemas de informação e a internet[1], como plataforma de ligação universal, como a rede das redes, ganham importância e um lugar quase omnipresente na vida quotidiana das sociedades. A internet provocou uma mudança de paradigma na comunicação e na transmissão de informação. Hoje todos somos produtores e recetores de informação. Isto significa, em teoria, que um utilizador ligado à "rede das redes", pode aceder a informações e recursos em qualquer uma dessas redes, utilizando-os e modificando-os de variadas formas, mesmo até de forma ilícita.

A globalização, tal como muitos outros fenómenos, para além das vantagens e benefícios, também tem inconvenientes e perigos, como o acentuar de desigualdades já existentes, o surgimento de sentimentos de injustiça e de exclusão, que poderão resultar em extremismos, violência e crime.

[1] Internet (acesso www) - Ligação ao conjunto de redes informáticas mundiais interligadas pelo protocolo TCP/IP – *Transmission Control Protocol/Internet Protocol*, onde se localizam servidores de informação e serviços (FTP, WWW, e-mail, etc.). (INE, 2012)

No mundo moderno continuam, no entanto, bem presentes fenómenos antigos. Fenómenos esses, ilegais e violentos, que surgem de surpresa, escolhendo como alvo principal a população, espalhando o terror e a incerteza e usando as mais modernas tecnologias de informação para obter a tão desejada e necessária mediatização. Falamos do Terrorismo, que apesar de antigo na sua génese, passou a estar gravado no subconsciente da generalidade das pessoas, tendo talvez o seu exponente máximo no atentado de 11 de Setembro de 2001 em Nova Iorque, que as televisões e outros meios de comunicação social se encarregaram de transmitir em direto por todo o mundo.

As organizações terroristas e o crime organizado são organismos "maleáveis", com grande capacidade de adaptação e que, fruto do seu poder económico, acompanham e utilizam as mais modernas tecnologias para planear, preparar e executar as suas ações, beneficiando das facilidades resultantes da globalização.

O conceito de terrorismo não é consensual, sendo possível encontrar uma miríade de definições. Vamos, para o presente trabalho, adotar a referida pela *North Atlantic Treaty Organization* (NATO) (2009), segundo o qual o terrorismo é "o uso ilegal da força ou da violência, ou a ameaça de uso, contra pessoas ou propriedades, na tentativa de coagir ou intimidar Governos ou sociedades para alcançar objetivos políticos, religiosos ou ideológicos". Esta definição poderá ser complementada com a defendida pelo Dr. Nuno Rogeiro (2004, p. 481), de que o terrorismo designa "um sistema, ou regime, baseado no medo provocado por atos de violência calculada, geralmente indiscriminada, de cariz eminentemente político, que não se confunde com a delinquência comum". São estes dois conceitos que enformam e enquadram o presente estudo.

O tema ora proposto "Terrorismo: a interrupção de sistemas", reveste-se da maior importância e utilidade para a compreensão de um fenómeno tão atual que irá, com toda a certeza, continuar a ocorrer no futuro, quer seja na sua "tradicional roupagem" de atentados bombistas, raptos ou assassínios, quer seja em modalidades mais sofisticadas, como sejam o ciberterrorismo e a utilização de armas de destruição massiva.

O objeto de estudo do presente trabalho foca-se no impacto que as ações terroristas têm na vida das pessoas e nos próprios Estados, quando são direcionadas e se centram na interrupção de sistemas, verificando se este tipo de ataque tem tendência a ganhar preponderância em relação aos restantes.

Quanto à dimensão geográfica do presente estudo, o enfoque residirá em Portugal e na realidade nacional, abordando, no entanto, os casos de alguns atores que atualmente se

encontram na "linha da frente" deste tipo de combate, nomeadamente a NATO, a União Europeia (UE) e alguns Estados que constituem estas organizações.

A investigação visa, como objetivo geral, verificar qual o impacto da interrupção de sistemas, provocada por ações terroristas nos Estados, focando-se temporalmente nos desenvolvimentos ocorridos após os acontecimentos do 11 de Setembro de 2001. O terrorismo, por ser um tema tão lato, carece de que, na presente situação, o estudo se limite especialmente às ações conducentes à interrupção de sistemas de informação e de comando e controlo.

A luta contra o terrorismo é, pelo menos internamente em Portugal, missão primordial das forças de segurança. No entanto, a ameaça terrorista, por ser difusa e encoberta, necessita da colaboração e cooperação entre todas as organizações do Estado, de forma a tornar eficiente o seu combate. Às FFAA Portuguesas incumbe participar nesta luta, em tarefas específicas e em situações cuja gravidade ultrapasse a capacidade de resposta das forças de segurança.

Quanto ao percurso metodológico, iremos utilizar o método hipotético-dedutivo, apoiados numa pesquisa bibliográfica e documental sobre o tema proposto, onde se procura visualizar a evolução e impacto deste fenómeno.

Assim, no capítulo das fontes, recorremos essencialmente a documentos oficiais, tanto nacionais como da UE, da NATO e dos Estados Unidos da América (EUA), bem como também a trabalhos e estudos publicados de diversos autores e ainda a artigos de revistas desta área do conhecimento. Estes documentos abordam tanto a problemática da interrupção de sistemas, o fenómeno do terrorismo, bem como as estruturas, organizações e sistemas para sua prevenção e combate, procurando argumentos contrários e diferentes perspetivas de análise. A recolha de informação foi complementada com a realização de entrevistas [2] a alguns estudiosos, militares e civis, de reconhecido prestígio e pela participação em conferências e seminários.

Para esta análise, pretendemos responder à **Questão Central** (QC), que orienta o trabalho: "**Que postura deverá Portugal adotar face à ameaça ciberterrorista com vista à interrupção de sistemas de informação?**"

[2] TCor Tm Viegas Nunes, professor de Mestrado em Guerra da Informação na Academia Militar (12Jan12); Prof. Dr. Marques Guedes, professor de Geopolítica do IESM (26Jan12); Dr. Rogério Bravo, Inspetor Chefe da Polícia Judiciária responsável pela área do cibercrime (30Jan12); Cor Tir António Tavares e Drª. Isabel Pais, Adjunto e Assessora do Vice-Presidente do Conselho Nacional de Planeamento Civil de Emergência (17Fev12); Engº Lino Santos, da Fundação para a Computação Científica Nacional (02Mar12).

Desta QC decorreram as seguintes **Questões Derivadas** (QD) a responder, após o teste das **Hipóteses** (H), que a seguir se enunciam:

QD1 – Qual a evolução do fenómeno terrorista e das formas de ataque por ele empregues?

H1 – O ciberterrorismo é uma adequação face ao avanço tecnológico presente na vida das sociedades modernas, por parte dos grupos terroristas, e configura uma mudança na sua estratégia de atuação.

QD2 - De que forma a interrupção de sistemas pode ter como consequência o colapso, mesmo que parcial, de um país?

H2 - A interrupção de sistemas pode ter consequências muito negativas para um país, caso estas sejam disruptivas, de grande alcance e por um período de duração suficiente para causar danos de elevada monta.

QD3 - Quais os principais aspetos que deverão constar numa Estratégia Nacional de prevenção e combate ao ciberterrorismo?

H3 - Portugal tem consciência do impacto deste tipo de ataque e deve desenvolver estruturas e sistemas de prevenção e proteção que privilegiem a complementaridade e colaboração entre os diferentes agentes envolvidos neste combate.

Este trabalho apresenta uma organização e conteúdo estruturados em três capítulos, terminando com as conclusões e recomendações.

Iremos começar por, no primeiro capítulo, caracterizar a problemática do terrorismo, procurando apresentar o seu estado da arte, abordando a sua origem e evolução, caraterização, tipologia e destacando o ciberterrorismo. No segundo capítulo pretendemos abordar o fenómeno da interrupção de sistemas, evidenciando a importância e o impacto deste na vida das populações e no funcionamento dos Estados, realçando o papel fundamental dos sistemas de informação e de comando e controlo. Posteriormente, no terceiro capítulo, analisaremos o sistema e estrutura de prevenção e combate existente em Portugal, apontando as especificidades relativas ao ciberterrorismo, bem como as estratégias de cibersegurança de alguns países de referência da NATO e UE, identificando quais os aspetos que a Estratégia Nacional de Cibersegurança (ENC) deverá abordar.

Entendemos assim, que a presente investigação possa ser um contributo para o conhecimento e melhor esclarecimento da temática, apresentando e apontando possíveis opções para o combate desta ameaça, as quais esperamos que possam vir a ter impacto em medidas de segurança a implementar futuramente.

1. O terrorismo

a. Caraterísticas principais

(1) Origens e evolução

As sociedades modernas têm ao seu alcance, de forma fácil e económica, uma infinidade de meios de comunicação social e de informação, através dos quais obtêm o conhecimento sobre o que se passa no mundo. Esta facilidade e rapidez de acesso à informação encurta distâncias, esbate fronteiras e cria nas pessoas a perceção de proximidade e de que vivemos hoje numa "aldeia global".

Existe um aspeto em comum entre uma aldeia real e uma "aldeia global" que é o facto de ambas terem vizinhos. No entanto, no caso da real os vizinhos conhecem-se, enquanto que na "aldeia global" não têm um conhecimento real sobre esses vizinhos (Silva, 2009, p. 139). A informação que nos é transmitida pelos meios de comunicação social, é sempre a visão e a interpretação de quem a transmite, moldando a opinião e perceção das pessoas, levando-as a terem ideias e compreensões que poderão ser erradas ou incompletas.

Convém ainda realçar que uma parte significativa da população mundial não tem, atualmente, acesso às modernas tecnologias de informação[3], tendo um leque mais limitado de fontes, o que facilita o controlo e a influência dos meios de comunicação existentes por parte das elites dirigentes e a consequente moldagem da perceção do mundo pela população que dirigem. É nos países em que estas condições se verificam, que mais facilmente florescem ideias e crenças deturpadas e se radicalizam posições que redundam em instabilidade e conflitos.

O terrorismo é um bom exemplo de como a perceção e a ideia que as pessoas têm sobre ele pode ser moldada e influenciada, pois, ao analisarmos as informações veiculadas pelos meios de comunicação social ao nosso dispor, deparamo-nos com uma miríade de notícias sobre o terrorismo, especialmente após o 11 de setembro, que nos poderia levar a pensar que estamos perante um fenómeno recente e exclusivo dos nossos dias, o que é falso. Trata-se de algo bem antigo, que "vem pelos séculos fora, tendo ganho especial ênfase com os anarquistas do final do Século XIX e princípios do Século XX " (Leandro, 2004).

[3] A população mundial atual é de mais de 7.000 milhões de pessoas e o número de utilizadores da internet é de 2.300 milhões (Worldometers, 2012).

A história do terrorismo é tão antiga quanto a vontade dos seres humanos em usar a violência para afetar a política. O *Sicarii* era um grupo judeu do primeiro século que matou inimigos durante a sua campanha para expulsar os governantes romanos da Judeia. O *Hashhashin* , cujo nome deu origem à palavra "assassinos", era uma seita secreta islâmica ativa no Irão e na Síria durante os séculos XI e XII (Zalman, s.d.).

A palavra "Terrorismo" entrou nas línguas europeias, com a Revolução Francesa de 1789. Nos primeiros anos da revolução, os Governos tentavam impor a nova ordem, em grande parte, através da violência. Como resultado, o primeiro significado da palavra "Terrorismo", conforme registrado pela *Académie Française* em 1798, foi de "sistema ou regra de terror ".

Durante o século XIX, o terrorismo passou por uma transformação importante, vindo a ser associado, como ainda é hoje, aos grupos não-estatais. Um desses grupos, o pequeno grupo de revolucionários russos *Narodnaya Volya*, em 1878-81, desenvolveu as ideias que se tornariam a imagem de marca do terrorismo subsequente em muitos países, a morte dos "líderes da opressão". O terrorismo continuou por muitas décadas a estar associado, principalmente, ao assassinato de líderes políticos e Chefes de Estado. Um bom exemplo deste tipo de prática foi a assassinato do arquiduque austríaco Ferdinand, em Sarajevo em 28 de junho de 1914, que serviu de catalisador específico para o eclodir da Primeira Guerra Mundial.

Na segunda metade do século XX, após a Segunda Guerra Mundial, o terrorismo ampliou a sua esfera de ação para além do assassinato de líderes políticos e Chefes de Estado. Entrava-se na época das descolonizações, e os movimentos terroristas (também chamados de movimentos de libertação) desenvolveram as suas atividades, muitas vezes com duas finalidades distintas: colocar pressão sobre as potências coloniais para apressar a sua retirada e, intimidar a população indígena para apoiar as suas reivindicações.

O terrorismo não terminou após as descolonizações nas décadas de 1950 e 1960, tendo continuado em muitas regiões, em resposta a circunstâncias diversas, passando os alvos agora a serem civis.

Quando em setembro de 1970, terroristas palestinianos sequestraram vários aviões e os desviaram para a Jordânia, e apesar de terem libertado os passageiros, esses atos foram vistos por muitos, tanto com fascínio como com horror. Em seguida, em setembro de 1972, mostrando uma clara determinação para matar, 11 atletas israelitas são assassinados, num ataque palestiniano, nos Jogos Olímpicos de Munique. Determinação essa que se tornaria ainda mais visível algumas décadas mais tarde, com os atentados suicidas. Em alguns dos

atentados suicidas havia um elemento novo que não tinha sido evidente anteriormente: o extremismo religioso islâmico.

Na década de 1990, uma nova face do terrorismo emergiu. Osama Bin Laden tornou-se líder do movimento islâmico, *Al-Qaeda*[4]. As suas declarações públicas eram uma mistura de extremismo religioso, desprezo para com os atuais regimes árabes, hostilidade face ao domínio dos EUA e insensibilidade quanto aos efeitos que as suas ações provocavam. Surgia assim, um novo tipo de movimento terrorista, com uma determinada causa, organizado em rede, que não se limitava a um único Estado e cujos apoiantes estavam dispostos a cometer suicídio para destruir os seus adversários (Roberts, 2002)[5].

(2) Descrição e tipologia

A dificuldade de definir o conceito de terrorismo "deriva da diversidade de motivos que mobilizam os terroristas, dos fins que prosseguem e dos métodos que empregam, combinado com o facto de que o terrorista, que alguns denunciam, é o lutador pela liberdade que outros prezam" (Dougherty & Jr., 2003, p. 495).

Uma vez que a definição deste fenómeno não é consensual, e existe uma enorme variedade de diferentes entendimentos sobre o termo, no presente trabalho iremos adotar o conceito da NATO, complementado pelo do Dr. Nuno Rogeiro, já referidos na introdução deste estudo.

O ataque terrorista caracteriza-se por ser realizado de surpresa, pela sua violência extrema e por ter como alvo preferencial a população, locais ou infraestruturas de utilização massiva, havendo enorme probabilidade de ocorrência de um elevado número de vítimas. Provoca o terror, o pânico e o medo constante, obrigando as pessoas a viverem em permanente sobressalto, condicionando o seu normal modo de vida.

Existem cinco alterações fundamentais que diferenciam aquilo que era o terrorismo antes e depois do 11 de Setembro: a cultura teocrática, que alavanca a predisposição para "morrer matando"; a estrutura organizacional fluida, de rede, que favorece a ligação com outras organizações e movimentos terroristas e que dificulta o seu aniquilamento; a imprevisibilidade; a perda da característica seletiva do alvo, que elege a população civil como alvo de excelência, e o facto de deixar de ser visto como um fenómeno de segurança

[4] Al-Qaeda significa em português "A Base".
[5] Em 2011, os EUA consideravam existir 49 organizações terroristas (U.S.Department of State, 2011).

interna para passar a ser encarado como um fenómeno internacional (Teixeira, 2009, p. 156).

O terrorismo é usado como forma de combater injustiças ou ilegitimidades sociais ou nacionais, fazendo uso das consequências chocantes que caracterizam a violência destas ações, explorando e maximizando todo o espectro de meios de comunicação disponível, tentando perder o seu carácter local (Mathias, 2009, p. 131).

Atualmente, o terrorismo deixou de ser visto como local ou regional, como acontecia na sua génese, passando a ser encarado como um fenómeno global. Podemos afirmar que a globalização chegou a todas as áreas das sociedades, incluindo as atividades ilegais e criminosas, como sejam o crime organizado e o terrorismo.

O terrorismo tem "uma organização específica, maleável, multicelular, servindo-se e servindo o crime organizado em grande escala, utilizando todos os recursos que a moderna tecnologia coloca à sua disposição" (Santos, 2009, p. 164). Segundo o Prof. Dr. Marques Guedes (2007, pp. 24,37), o aumento da pressão por parte dos Estados impeliu as organizações terroristas a adotarem uma organização em rede, como forma de garantir a sua segurança e aumentar a sua resiliência, pois verifica-se uma superioridade, quando em confronto, das redes policentradas sobre as estruturas hierárquicas. As formas de organização, recrutamento e financiamento são apresentadas no Apêndice 2 deste trabalho.

O objetivo terrorista é coagir um Governo a decidir de acordo com as suas exigências. Os terroristas podem "ser motivados pela vingança de injustiças históricas, pela demonstração de ódio pelo sistema capitalista ou pela fúria fundamentalista contra os infiéis ou hereges. A loucura calculada do terrorista consiste precisamente no facto de as vítimas terem pouco ou nada que ver com a causa e terem ainda menos capacidade de cumprir as exigências requeridas" (Dougherty et al., 2003, p. 495). A sequência das suas ações é a descrita no Apêndice 3 a este trabalho.

Como existe um leque alargado de tipificação do terrorismo, no presente trabalho vamos adotar a sistematização defendida por Mendoza, Pavolka e Niznansky (2006, pp. 14-16), que se foca na análise das motivações e no local de origem e dimensão dos seus efeitos, para classificar a diferente tipologia do fenómeno terrorista. Assim, o terrorismo apresenta a seguinte tipologia:

- Dependendo da motivação:
  - Terrorismo Secular: geralmente caracterizado por ser composto por um número diminuto de pessoas, com uma estrutura altamente hierarquizada, apoiada por ideias nacionalistas extremistas, que perseguem o objetivo estratégico de forçar a

ocorrência de mudanças políticas na direção que desejam. São exemplos grupos como o *Euskadi Ta Askatasuna* (ETA), ou o *Irish Republican Army* (IRA).

  - Terrorismo Religioso: composto por um grande número de seguidores, que não tem uma estrutura hierárquica claramente definida, cuja justificação moral para a violência é a religião. Executam ataques em grande escala e os alvos escolhidos têm valor simbólico. Não temem a perda do apoio da população realizando os ataques sem impedimentos. O exemplo mais claro desta tipologia é o chamado terrorismo islâmico ou islamita.

- Dependendo do local de origem e dimensão dos seus efeitos:
  - Terrorismo Endógeno ou Nacional: tem origem interna e as ações são limitadas geograficamente a esse Estado, cuja população procura aterrorizar e cujas estruturas visa destabilizar. São exemplos grupos como a ETA, IRA ou as Forças Populares 25 de Abril (FP 25).
  - Terrorismo Exógeno ou Transnacional: tem origem externa e não está ligado a nenhum conflito local específico. Parece inspirado por uma motivação global, estando disposto a atacar qualquer país e a usar a violência ilimitada. É exemplo desta tipologia a *Al-Qaeda*.

Além desta tipologia, existem outras formas de classificar o terrorismo de acordo com o tipo de armas que utilizam nos seus ataques (terrorismo nuclear, biológico, químico, e radiológico (NBQR), ou ciberterrorismo), no entanto, estas formas de terrorismo acabam por ser acomodadas nas categorias definidas na classificação anterior.

b. Ciberterrorismo

Os sistemas de informação são um dos elementos fundamentais que caracterizam a atualidade. Esta Era de importantes mudanças, embora tenha gerado oportunidades de progresso e desenvolvimento, também tem conduzido frequentemente a situações de instabilidade e originado conflitos que colocam em causa os objetivos últimos dos Estados: garantir a segurança, a prosperidade e o bem-estar social do seu povo (Couto, 1988, p. 23).

É neste contexto que o ciberterrorismo se reveste da maior acuidade, como pode ser constatado nos exemplos recentes dos ataques de 2007 na Estónia, de 2009 na Geórgia, no caso *Wikileaks* ou nos ataques do grupo *Lulzsec* Portugal, efetuados em novembro do último ano.

(1) Caraterização e objetivos

Fruto da enorme evolução tecnológica e da crescente automatização de todas as áreas de atividade das sociedades atuais, o "ciberespaço surge como um novo espaço virtual de interação económica, social e cultural. As sociedades industriais, especialmente as que vivem num sistema de mercado livre e aberto, apresentam uma grande dependência relativamente às redes e sistemas de informação que estão na base do seu processo de geração de riqueza e de bem-estar social" (Nunes, 2009).

Devido à crescente digitalização, a internet e as redes de computadores têm hoje uma importância vital. A internet, rede planetária que surgiu para fins militares no final da década de 1950 (Perles, s.d.), que se "civilizou" e que nos dias de hoje está profundamente divulgada e acessível a todos, sendo um meio indissociável e indispensável da vida moderna, é constituída por uma rede de comunicações transnacional que permite a troca de informação e a aquisição de bens e serviços[6].

É a crescente importância da internet e dos sistemas de informação que fazem surgir os termos cibercrime, ciberguerra, ciberataque, cibersegurança e ciberterrorismo, levando os países e organizações a preocuparem-se e prepararem-se para esta realidade, criando estruturas e procedimentos de defesa e de combate para lhes fazer face.

Segundo Dorothy Denning (2000), o ciberterrorismo é a convergência entre o ciberespaço e o terrorismo. São ataques ilegais contra os computadores, redes e as informações neles armazenadas, efetuados para intimidar ou coagir um Governo ou o seu povo, em prol de objetivos políticos ou sociais. Um ataque para ser qualificado como ciberterrorista deve resultar da violência contra pessoas ou bens ou, pelo menos, causar dano suficiente para gerar medo. Ataques sobre as infraestruturas críticas (IC) que afetem gravemente a vida de pessoas, que causem explosões ou perdas económicas graves são exemplos de ataques ciberterroristas. Ou seja, o ciberterrorismo é a utilização do ciberespaço para alcançar os mesmos objetivos ou objetivos semelhantes do "terrorismo tradicional".

O cibercrime é um ato praticado contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a sua utilização fraudulenta. Incluem acesso e interceção ilegítima, interferência em dados e sistemas, uso abusivo de dispositivos, falsidade e burla informática, infrações relacionadas

[6] Em 2010 o número de utilizadores mundial da internet rondou os 2.100 milhões e em Portugal, no ano passado, 63,7 % dos agregados domésticos já tinham ligação à internet.

com pornografia infantil e violação do direito de autor (Conselho da Europa, 2001). Segundo a INTERPOL (2011), é uma das áreas de maior crescimento da criminalidade.

(2) Recrutamento e organização

O ciberespaço tem vindo a constituir um autêntico campo de batalha digital, onde indivíduos, organizações e até mesmo Estados têm executado ações ofensivas e defensivas, de forma a atingirem os seus objetivos.

É neste "novo" campo de batalha que o ciberterrorismo prolifera e, "ao contrário das guerras convencionais que envolvem homens fortemente armados, uma grande estrutura de defesa e segurança, esta é uma guerra moderna sem rosto, sem identidade e sem as fronteiras físicas do Estado" (Dias, 2011). Algumas das principais características dos ciberataques são que podem ser conduzidos remotamente, no anonimato, são baratos, não exigem o uso de explosivos nem suicidas e são de difícil prevenção e combate porque podem ser efetuados de qualquer parte do mundo.

Existem três formas básicas de ciberataques: ataques sobre a confidencialidade dos dados, que abrange qualquer aquisição não autorizada de informações; ataques sobre a integridade da informação, que inclui a sabotagem de dados com objetivos criminosos, políticos ou militares e os ataques sobre a disponibilidade de computadores ou recursos de informação. Esta terceira forma tem como objetivo evitar que os utilizadores autorizados tenham acesso aos sistemas ou aos dados de que necessitam para executar determinadas tarefas. As ações que concretizam este objetivo são comumente referidas como negações de serviço (*denial-of service* - DoS)[7] e abrangem o tráfego de rede ou ataques físicos a computadores, bases de dados e às redes que os ligam (Geers, 2011, p. 21).

Os métodos usados são muito variados e podem incluir: ataques para invadir ou para obter o controlo sobre a rede; vírus de computador e *worms*[8] que modificam e destroem informações ou prejudicam o funcionamento dos sistemas dos computadores; bombas lógicas que se instalam nos sistemas operativos dos computadores e permanecem em hibernação até serem acionadas, causando a destruição dos sistemas hospedeiros e,

[7] Para a coordenação e execução deste tipo de ataque, são utilizadas as denominadas Botnets. Botnet é a designação dada a um conjunto de bots sobre um mesmo comando, e um bot, diminutivo de robot, é um utilitário concebido para simular ações humanas, em geral numa taxa muito mais elevada do que seria possível para um editor humano sozinho. Os computadores infetados utilizados nestes ataques podem estar localizados em qualquer parte do mundo e o seu proprietário não sabe que este está corrompido e que está a ser utilizado no ataque.

[8] Vírus que se propagam de forma independente e destroem os sistemas operativos.

ainda, "*trojans*" que permitem a execução de certas ações sem o conhecimento do proprietário do sistema comprometido (Hawks, s.d.).

Embora existam alguns grupos ciberterroristas "puros", a grande maioria deriva de grupos terroristas já reconhecidos. Os atores do terrorismo convencional (*Talibans*, ETA, IRA, etc.) podem contratar *hackers*[9], recorrer à conversão de alguns *hackers* às suas ideologias ou podem criar os seus próprios *hackers*. No entanto, nem sempre é fácil ao grupo terrorista recrutar, no seu próprio seio, *hackers* e treiná-los, pelo que parece mais aceitável a primeira alternativa, ou seja, contratá-los (Batista, et al., s.d., p. 34).

É importante distinguir o *hacking* e o hacktivismo do ciberterrorismo. O *hacking* são atividades realizadas *on-line* e de forma encoberta, que procuram revelar, manipular ou explorar vulnerabilidades nos sistemas operativos dos computador e outros *softwares*. A distinção entre estes conceitos nem sempre é fácil, tornando-se ainda mais difícil quando os grupos terroristas recrutam ou contratam *hackers*, transformando-os em ciberterroristas. Esta transição pode ser motivada por dinheiro ou prestígio. O hacktivismo pode ser definido como o uso ilegal ou de legalidade duvidosa, mas não violenta, de ferramentas digitais com objetivos políticos. Incluem invasões de *sites*, negação de serviços, roubo de informações e sabotagens. É usado para promover ideias políticas, a liberdade de expressão, os direitos humanos ou informações éticas. Defende o acesso à informação como um direito humano básico (Hawks, s.d.). Podem ser considerados exemplos de hacktivismo, as ações desencadeadas recentemente pelos grupos *Wikileaks* ou *Anonymous*, se bem que esta catalogação possa ser controversa e existam países que as consideram como terroristas ou pelo menos criminosas. São dois grupos que defendem o acesso à informação sem restrições e a utilização da internet sem custos, e cujas ações têm colocado em causa, não só a credibilidade dos sistemas de segurança de Estados e de grandes empresas ou organizações, como também os factos revelados têm provocado polémica, embaraço e comprometimento das instituições visadas.

O tipo de pessoa que se dedica ao *hacking* parece estar a mudar. No início eram principalmente jovens estudantes, curiosos, que o faziam sobretudo por diversão, mas nos

[9] O significado original do termo *hacker* era até bastante positivo. Significava um utilizador de tecnologia muito inteligente, capaz de modificar *hardware* ou *software*, com a finalidade de atingir os seus limites e até ultrapassá-los, conseguindo uma utilização para além da que os seus inventores tinham pretendido. Ao longo do tempo, no entanto, com a alteração dos seus objetivos que deu origem à sua criminalização, levou à alteração e à decadência do sentido original do termo (Geers, 2011, p. 20).

últimos anos verifica-se que muitos são excelentes programadores, com idades a rondar os 30 anos.

Os terroristas, além de utilizarem o ciberespaço para atividades estritamente ciberterroristas, utilizam-no também para facilitar e complementar as formas tradicionais de terrorismo, como por exemplo os atentados, potenciando, de forma exponencial, os seus efeitos, incluindo os mediáticos. Usam a internet como meio de comando e controlo, comunicando e passando informações sobre possíveis alvos, utilizando mensagens de correio eletrónico cifradas, e também para fins propagandísticos, publicitando a sua causa com o objetivo de angariar fundos e recrutar seguidores. Utilizam não só os *websites* já disponíveis, como criam *websites* para as próprias organizações. Uma sistematização das ciberameaças do nosso século poderá ser consultada no Apêndice 4 a este trabalho.

Segundo Thornton (2010), a maioria dos 45 grupos designados como organizações terroristas estrangeiras pelo Departamento de Estado dos EUA, usam a internet como principal ferramenta para divulgação e recolha de informações e recrutamento. Entre 1998 e 2006, o número de *websites* apoiados por terroristas aumentou de 12 para mais de 4.300, recebendo os mais populares, dezenas de milhares de visitas por mês de todo o mundo. Incorporam tecnologia de ponta semelhante à usada nos *websites* das grandes empresas ou organizações. Por exemplo, o *site* do Hamas inclui um motor de busca, refere qual a missão, tem uma secção de novidades e uma página de questões frequentes. Estes *websites* têm quatro objetivos principais: disseminar informação[10], obter informação[11], organização[12] e recrutamento[13].

(3) Evolução e impacto

A história é muitas vezes marcada por revoluções científicas e tecnológicas. Presentemente, estamos no meio da chamada "Revolução da Informação". Segundo a *Central Intelligence Agency* (CIA) (2011), em 2010, houve 2.100 milhões de utilizadores de internet no mundo.

[10] São usados não só para espalhar mensagens radicais, mas também para ganhar credibilidade mantendo os *websites* bem conservados.

[11] Através de motores de busca, listas de distribuição de email, salas de *chat*, grupos de discussão e podem ser cruciais para o desenvolvimento de operações terroristas obtendo informações sobre horários e localização dos alvos, sobre transportes, prédios públicos e aeroportos.

[12] A estrutura organizacional dos grupos terroristas torna-se cada vez mais em rede com níveis hierárquicos cada vez mais esbatidos, facilitando a comunicação, o planeamento e exigindo menos recursos.

[13] Os grupos terroristas dispõem de um campo de recrutamento que era anteriormente inacessível através dos meios tradicionais, passando o recrutamento a ser a nível mundial e a baixo custo.

Os países economicamente desenvolvidos, ou em vias de desenvolvimento, dependem cada vez mais dos sistemas de informação e das comunicações. Os seus principais sistemas, designadamente os sistemas financeiros, de saúde, de comunicações, de segurança e defesa, entre outros, são geridos por sistemas informáticos cada vez mais complexos. O ciberespaço está constantemente sob ameaça.

A acessibilidade, o anonimato e a omnipresença da internet criaram oportunidades para as organizações criminosas e para o terrorismo transnacional, podendo causar enormes estragos. Os exemplos abundam, tais como: em 1995, um estudante britânico de 16 anos de idade invadiu os arquivos do Governo dos EUA e fez o *download* de informações sensíveis relativas à investigação de armas balísticas da Coreia do Norte; em 2000, uma tentativa de desviar 400 milhões de dólares de fundos da UE foi impedida, devido a uma informação de um dos conspiradores[14]; o apoio financeiro dos atentados de 2002 em Bali, na Indonésia, foi obtido através de fraudes *on-line* de cartões de crédito; em 2005, um jovem de Massachusetts foi responsável pelo roubo de informações pessoais e por criar o pânico com ameaças de bomba; em 2007, os serviços de segurança britânicos, o gabinete do primeiro-ministro francês e da chanceler alemã, queixaram-se de que teriam sido alvo de intrusões eletrónicas por parte da China; ainda no mesmo ano, talvez o ataque mais conhecido seja o que sofreu a Estónia, presumivelmente a partir da Rússia, ataque esse que paralisou por completo o país durante semanas; em 2009, investigadores canadianos descobriram um sistema de espionagem implantado nas redes governamentais de 103 países (Jarmon, 2011, pp. 111,112). No Apêndice 5 poderão ser consultados alguns dos principais ciberataques desde 2002.

A lista de potenciais alvos parece interminável. As tendências sugerem que todos os potenciais alvos estão cada vez mais ligados à internet e que utilizam como sistemas de informação os sistemas *Windows* ou *UNIX*, mais baratos, mais fáceis de usar, mas também mais fáceis de atacar. Atualmente, o mais sofisticado *worm* dá pelo nome de *Stuxnet* e tem como alvo IC que utilizem os sistemas *Supervisory Command and Data Acquisition* (SCADA). Os sistemas SCADA são utilizados para controlo industrial ou em infraestruturas, tais como, fábricas, produção de energia, distribuição e tratamento de água, oleodutos, distribuição de energia elétrica, etc.

Com o aumento da importância da internet, houve a necessidade da segurança informática passar do nível tático para o nível estratégico. O motor desta mudança foi a

[14] Os fundos seriam lavados através de vários bancos *on-line*, incluindo o banco do Vaticano.

constatação de que a combinação das vulnerabilidades dos computadores e a interligação mundial tinham colocado em risco as IC dos países (Geers, 2011, pp. 24-29). Foi esta constatação que levou a UE a estabelecer uma convenção do cibercrime em 2001, à qual Portugal aderiu, que levou a NATO a alterar o seu conceito estratégico em 2010, passando a considerar os ciberataques como uma ameaça que urge combater, (Abrial, 2011) e que levou ainda os EUA a criar, em 2010, um comando específico para o ciberespaço (USCYBERCOM).

O ciberterrorismo é uma ameaça global que exige uma defesa e um combate igualmente global. Como referiu o Brigadeiro-General Brundidge (2011), numa conferência no Instituto de Defesa Nacional em dezembro de 2011, o ciberespaço está em todo o lado. Todos os setores, público e privado, coexistem no mesmo ciberespaço, sendo essencial o trabalho em conjunto, a colaboração e a partilha de informação entre todos os setores para uma cibersegurança eficaz. Os líderes dos países têm de estar conscientes da importância destas ameaças, da necessidade de formar quadros e de possuir organismos que lhes deem luta, de que não é possível defender tudo nem fazer face a todas as ameaças, e que, por isso, é necessário definir prioridades e focar-se no essencial.

c. Síntese conclusiva

O terrorismo está atualmente omnipresente na vida quotidiana das populações dos diferentes países, influenciando de forma vincada muitos dos diferentes setores das sociedades modernas. No entanto, e ao contrário do que poderemos ser levados a pensar, a sua origem é bastante antiga, tendo a sua evolução acompanhado a própria evolução da humanidade, adaptando-se e, inclusivamente, incorporando os fatores marcantes dessa mesma evolução.

A globalização expandiu o terrorismo, deixando este de ser local ou regional e passando a ser transnacional. O terrorismo transnacional é de tal maneira difuso que origina o aparecimento de um leque variado de definições, apresentando como caraterísticas principais a sua imprevisibilidade, a extrema e indiscriminada violência empregue, a população como o alvo preferencial e os seus objetivos eminentemente políticos, religiosos ou ideológicos.

Os sistemas de informação são um dos componentes basilares que caracterizam a atualidade, assumindo a internet um papel fundamental na vida da maioria das pessoas, das empresas e dos organismos estatais de todos os países. Hoje, todos os principais sistemas de um país, quer sejam económicos, financeiros, de saúde, de comunicações, de

transportes, de produção e distribuição de energia e água, de segurança ou defesa, são geridos ou dependem, de alguma forma, de sistemas informáticos.

É neste contexto, de crescente importância e dependência dos sistemas de informação e controlo, que surge o ciberterrorismo e que a capacidade disruptiva dos seus ataques ameaça, agora, a segurança nacional e internacional. Esta nova arma, mesmo quando não é a principal arma usada, teve, com toda a certeza, grande importância numa das fases do processo, sendo a sua utilização frequentemente conjugada com as tradicionais, de forma a aumentar a eficiência e eficácia do ataque. Não consideramos que os objetivos da ameaça terrorista tenham mudado com o ciberterrorismo, mas esta nova arma veio alterar a sua estratégia. Segundo Cabral Couto (1988, p. 209), a estratégia é "a ciência e a arte de desenvolver e utilizar as forças morais e materiais de uma unidade política ou coligação, a fim de se atingirem objetivos políticos que suscitam, ou podem suscitar, a hostilidade de uma outra vontade política". Deste conceito poderemos inferir, como elementos chave da estratégia, as forças morais e materiais, a forma como estas são empregues e os objetivos políticos que se pretendem alcançar, conjugados num determinado ambiente. Excetuando os objetivos das organizações terroristas, todos os restantes elementos se alteraram, pelo que entendemos estarem reunidas as condições que consubstanciam uma mudança estratégica. Os ataques terroristas visando a interrupção de sistemas, independentemente do método utilizado, ganharão preponderância e as IC dos países estão agora em risco, devendo o ciberespaço passar a ser considerado como uma nova e importante componente. Desta forma, confirmamos a **H1**, de que o ciberterrorismo é uma adequação face ao avanço tecnológico presente na vida das sociedades modernas, por parte dos grupos terroristas e configura uma mudança na sua estratégia de atuação, respondendo assim à **QD1**: "Qual a evolução do fenómeno terrorista e das formas de ataque por ele empregues?"

2. Interrupção de sistemas

a. Os sistemas nas sociedades modernas

Segundo o Prof. Dr. Manuel Meireles (2001, p. 23), um sistema é um conjunto de partes interdependentes que juntas formam um todo unitário. Tendo por base este conceito e fazendo uma rápida análise do mundo que nos rodeia e da sociedade em que vivemos, facilmente constatamos que tudo faz parte de um sistema, sistema esse que, por sua vez, é uma parte de um outro sistema mais amplo (Gouveia & Ranito, 2004, p. 26). A nossa sociedade é um sistema complexo formada por muitos outros sistemas, interligados e interdependentes, que interagem entre si de forma organizada, procurando uma situação de equilíbrio. Esta ideia pode ser igualmente verificada a nível global. Acontece, frequentemente, existirem fatores que põem em causa o equilíbrio do sistema, que, por estar profundamente interdependente com outros sistemas a montante e a jusante, criam um desequilíbrio em cascata, podendo não ser fácil de recuperar, originando situações de crise mais ou menos graves.

Uma das caraterísticas da globalização, alcançada em grande parte pela vertiginosa evolução tecnológica, foi precisamente facilitar e amplificar esta dependência. Hoje, todos os países fazem parte de uma teia de relações e interações que, de diferentes formas e a níveis de dependência diferenciados, fazem com que um determinado acontecimento num país possa ter repercussões graves, não só a nível interno, como também noutros países, mesmo que distantes geograficamente.

Nesta "interdependência complexa, as sociedades interagem de muitas formas." Quando a interação atravessa fronteiras fora do controlo dos órgãos de política externa, é chamada de relações transnacionais. Relações que englobam "a migração de populações, a transferência rápida de capital,… o tráfico ilegal de armas e de estupefacientes e determinadas formas de terrorismo" (Jr., 2002, p. 245).

Existem, no entanto, algumas partes constituintes desta vasta engrenagem que, pelas suas caraterísticas e alcance, são mais importantes que as outras, são as chamadas IC. As infraestruturas críticas nacionais (ICN) não são mais do que componentes, sistemas ou parte destes, situados em território nacional, essenciais para a manutenção de funções vitais para a sociedade, saúde, segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções (Assembleia da República, 2011). Sabendo que deverão existir mecanismos e procedimentos que protejam todos os sistemas (grandes e pequenos) e seus

constituintes, é lógico que, caso haja a necessidade de definir prioridades de proteção, a prioridade deverá ser dada às IC já referidas.

É precisamente este o procedimento efetuado pelos Estados, numa época de grande e rápida mudança e inovação, em que a imprevisibilidade, multiplicidade e quantidade de ameaças e riscos é enorme, tornando impossível garantir o mesmo nível de proteção a todas as infraestruturas. Não sendo possível proteger tudo, há que identificar e definir o que é prioritário e concentrar esforços na proteção do que é realmente essencial.

Como refere Rocha (2007-2008, p. 134), com o qual concordamos, "a proteção das infraestruturas críticas deverá ser uma responsabilidade partilhada pelo sector público, pelo sector privado e por todos os cidadãos, sendo que só uma intervenção conjunta poderá fazer face ao enorme espectro de ameaças e riscos a que estão sujeitas aquelas infraestruturas, bem como preparar uma resposta adequada em caso da ocorrência de crises".

Foram acontecimentos como os atentados terroristas de 11 de setembro de 2001 em Nova Iorque, de 11 de março de 2004 em Madrid, 7 de julho de 2005 em Londres, bem como os apagões em 2003 nos EUA e em 2006 na Alemanha, ou os acontecimentos ocorridos na Estónia em 2007, que vieram consciencializar os Estados para a necessidade da Proteção de Infraestruturas Críticas (PIC). "Embora o terror seja atualmente o principal catalisador das atuais preocupações, é hoje internacionalmente reconhecido que as consequências da disrupção das IC são independentes do agente disruptor, pelo que a abordagem da sua proteção deve ser holística, dirigida a qualquer ameaça plausível, seja qual for a sua natureza" (Pais, et al., 2007). No entanto, como refere o Prof. Dr. Marques Guedes (2012), o terrorismo é, sem sombra de dúvida, uma das mais importantes ameaças ao equilíbrio destes sistemas e destas infraestruturas, podendo ter um enorme impacto na sua interrupção.

A UE (2010), tendo plena consciência da importância e vulnerabilidades das suas infraestruturas, bem como da necessidade da sua proteção, deu início a um conjunto de procedimentos no sentido de que fossem tomadas medidas pelos Estados Membros (EM). Assim, em Junho de 2004, o Conselho Europeu solicitou à Comissão que elaborasse uma estratégia global de reforço da PIC, tendo sido publicada, em Outubro desse ano, a Comunicação "proteção das infraestruturas críticas no âmbito da luta contra o terrorismo". O projeto da Comissão visa propor um Programa Europeu de Proteção das Infraestruturas Críticas (PEPIC) e uma Rede de Alerta para as Infraestruturas Críticas da União Europeia (RAIC).

O PEPIC é composto por: um procedimento de identificação e designação das Infraestruturas Críticas Europeias (ICE), uma abordagem comum para avaliar a necessidade de melhorar a sua segurança, medidas destinadas a facilitar a sua melhoria (um plano de ação, uma RAIC, grupos de peritos de PIC, procedimentos de partilha de informações, identificação e análise da interdependência), apoio aos EM (a seu pedido) e por último, planos de intervenção (União Europeia, 2010).

A 12 de dezembro de 2006, a Comissão apresentou uma proposta de Diretiva relativa à identificação e designação das ICE e à avaliação da necessidade de melhorar a sua proteção. O Programa da UE sobre "Prevenção, preparação e gestão das consequências em matéria de terrorismo e outros riscos relacionados com a segurança" foi adotado a 12 de fevereiro de 2007 (União Europeia, 2010). Por último, a 08 de dezembro de 2008 foi finalmente adotada a Diretiva já anteriormente referida (Diretiva 2008/114/CE) (Pais et al., 2010, p. 32).

Segundo a Comissão Europeia, existem três fatores que identificam as IC: o alcance (extensão da área geográfica afetada), a magnitude (grau do impacto ou da perda) e os efeitos no tempo (Rocha, 2007-2008, p. 134). Considera-se ICE aquela, que situada em território nacional, se for perturbada ou destruída, terá um impacto significativo em, pelo menos, mais um EM da UE, sendo este avaliado em função de critérios transversais, incluindo os efeitos resultantes de dependências intersectoriais em relação a outros tipos de infraestruturas (Assembleia da República, 2011).

Procurando acompanhar a realidade europeia e tendo em conta o "papel do Estado como promotor e regulador da segurança como bem público", o Conselho Nacional de Planeamento Civil de Emergência (CNPCE) coordenou o desenvolvimento do Programa Nacional de Proteção de Infraestruturas Críticas (PNPIC) (Pais et al., 2009, p. 39). Este programa é constituído por três fases: Fase 1 - identificação e classificação das ICN; Fase 2 - estudo e difusão de medidas eficientes para reforço da sua proteção e por último, Fase 3 - implementação de medidas e monitorização do risco (Pais et al., 2009, p. 39), (Alberto, 2011, p. 16).

A Fase 1 já foi concluída, tendo sido identificadas cerca de 12.000 infraestruturas, que foram reunidas numa base de dados segura e integrada num sistema de informação geográfica. Segundo o Sr. Cor Tavares e a Dra. Isabel Pais (2012) do CNPCE, destas 12.000 infraestruturas, cerca de 2,5% são consideradas ICN, ou seja, em Portugal foram identificadas cerca de 300 IC. Como resultado desta fase, releva-se que mais de 65% das ICN localizam-se em zonas de risco sísmico, encontrando-se algumas em zonas de elevado

risco de incêndio florestal ou em leitos de cheia (Pais, et al., 2007), o que é revelador das fragilidades e riscos que estas tão importantes infraestruturas possuem e correm. No Anexo A encontra-se elencada a sistematização seguida pela UE e por Portugal.

A Fase 2 está em desenvolvimento, estando a ser utilizada uma abordagem holística *"all-hazards approach"* e uma setorial, tal como na Diretiva Europeia, tendo sido identificadas como ameaças prioritárias, a sísmica e a cibernética (Pais et al., 2010, p. 35).

Relativamente à Fase 3, existem já algumas medidas de monitorização do risco, mas não foram implementadas medidas de reforço da proteção das ICN, uma vez que ainda não está concluída a Fase 2 (Mascarenhas, 2012). Devemos ter bem presente que o PNPIC é um programa dinâmico, de profunda inter-relação entre as suas fases, não sendo possível afirmar que está concluído, dado que está em contínua evolução, avaliação e correção.

Sendo certo que é competência e responsabilidade do Estado garantir a segurança dos seus cidadãos, bem como dos seus bens, é igualmente um facto que a maior parte das IC estão nas mãos dos privados, devendo o Estado estimular a adoção, por parte destes, de medidas que as protejam. É esperado, por parte do setor privado, uma resposta eficiente do Estado em situações de crise, bem como o auxílio à recuperação económica dos setores atingidos, o que poderá originar uma certa negligência e desinvestimento por parte destes, em questões de segurança. Esta postura deverá ser contrariada, sendo feita a aposta na prevenção em detrimento da reação, devendo cada uma das partes assumir a sua parte das responsabilidades (Rocha, 2007-2008, p. 141).

É crucial, para uma eficaz segurança das IC, a procura de soluções com claros benefícios para as partes envolvidas, percebendo todos que o que está em jogo justifica, de forma inequívoca, os investimentos a realizar, contrariando a natural resistência dos proprietários a investir em segurança. Como referência, podemos indicar o valor exposto num estudo efetuado pela McAfee (feito a empresas de IC em sete setores de 14 países), de seis milhões de dólares por dia, como custo de paralisações motivadas por grandes ataques cibernéticos. Sendo que, para além do prejuízo monetário que é de elevada monta, é referida, como a perda mais temida, o dano na reputação e a perda de informações pessoais dos clientes (Baker, et al., 2010, p. 3). Desta feita, a cooperação e partilha de responsabilidades e custos de investimentos são a base essencial para o aperfeiçoamento e implementação de políticas de proteção e reforço da segurança das IC (Pais, et al., 2007).

A partilha, a confiança e a cooperação apresentam-se assim como elementos indispensáveis, para que seja possível alcançar eficiência e eficácia na proteção das IC.

A realidade de hoje apresenta uma multiplicidade de ameaças e riscos tão elevada, que a sua prevenção e combate não poderá ser concretizada, em exclusivo, por apenas uma ou outra entidade, sendo fundamental colocar-se de lado as chamadas "quintas". "Os desafios de segurança a que estamos todos sujeitos não se compadecem com estes jogos de poder" (Amaral, 2008, p. 58).

O CNPCE encontra-se em processo de extinção[15] e as suas competências relativas ao PNPIC serão transferidas para a Autoridade Nacional de Proteção Civil (ANPC) (Mascarenhas, 2012).

b. Os sistemas de informação e de comando e controlo

A informação é fundamental na atualidade, estando presente em qualquer decisão quotidiana. Qualquer organização, independentemente da sua grandeza ou ramo de atividade, depende de informação para prosseguir o seu trabalho e atingir os seus objetivos. Sendo um facto que, nas sociedades modernas, a informação ocupa um lugar central, esta situação origina a necessidade de existir numa organização a estrutura apropriada para recolher, armazenar, processar e distribuir essa informação, tornando-a disponível a quem dela necessita e, no momento oportuno.

Assim, entende-se por sistema de informação o somatório de componentes interligados que trabalham em conjunto para recolher, processar, armazenar e disseminar informação para apoio à tomada de decisão, coordenação, controlo, análise e visualização dessa informação numa organização (Laudon et al., 2002). Quando estes sistemas são usados para difundir e implementar a decisão, passam a ser também sistemas de comando e controlo.

É antiga a expressão de que informação é poder. Esta interdependência não constitui em si uma novidade, mas sim os reduzidos custos motivados pela revolução da informação. Revolução que alude aos enormes e rápidos desenvolvimentos tecnológicos, quer de *hardware*, quer de *software*, e consequente redução de custos da sua operação. "No próximo século é previsível que a tecnologia da informação, em sentido lato, venha a constituir o recurso de poder mais importante" (Jr., 2002, pp. 248-251).

Os sistemas de informação, ao contrário do que poderemos ser levados a pensar, como estrutura de apoio à tomada de decisão, já existem há muito tempo e um claro exemplo disso mesmo é o caso das FFAA. O incremento da complexidade da gestão das

[15] n.º 3 do Artigo 42º do decreto-lei n.º 126-A/2011 – Lei Orgânica da Presidência do Conselho de Ministros - de 29 de dezembro.

forças e da conduta das operações, originou a necessidade de implementar medidas e processos para auxiliarem o comandante na tomada de decisão. Sendo logicamente, um processo evolutivo, que tem acompanhado o desenvolvimento tecnológico e que tem vindo a ser influenciado por este.

Hoje em dia, o computador é uma das tecnologias mais populares e eficazes disponíveis para tratar a informação e para implementar e controlar as decisões tomadas. Evidentemente que existem outras tecnologias, mas nenhuma apresenta um potencial tão marcante e influenciador como o computador. As organizações não só estão a ser transformadas pela máquina como a própria forma de lidar com a informação também está a mudar. Os objetivos principais dos sistemas de informação são "minorar as restrições impostas pela existência de fronteiras, proporcionando os mecanismos possíveis para suporte ao fluxo de dados e informação, congregando os esforços dos vários componentes da organização – subsistemas – e permitindo o funcionamento do sistema como um todo, inclusivamente no relacionamento com o mundo exterior". Fazem parte dos sistemas de informação não só a tecnologia, mas também os recursos humanos e a forma como estes organizam as suas atividades (Gouveia et al., 2004, pp. 9, 27 e 30).

Apesar de toda a evolução tecnológica e dos avançados meios ao dispor das organizações, os recursos humanos continuam a ser o seu principal ativo. No entanto, é também uma evidência que as Tecnologias de Informação e Comunicação (TIC) têm vindo progressivamente a ocupar um lugar de destaque em todos os sectores da sociedade e que a dependência da internet é hoje uma realidade inequívoca. Esta tem uma utilização transversal, sendo por seu intermédio que muito do comércio e das transações financeiras são efetuadas, bem como grande parte do fluxo de informação mundial. A rapidez, a facilidade de utilização, a capacidade de comunicação e o seu baixo custo são as suas principais características e as suas vantagens, que podem, simultaneamente, ser exploradas por pessoas bem ou mal intencionadas.

A informática tem uma grande importância na gestão e operação das mais importantes infraestruturas, pois o seu baixo custo, associado aos ganhos de produtividade e eficiência, originou a sua implementação e expansão em larga escala, sendo utilizada na maior parte das atividades dos sectores críticos da nossa vida (Santos, 2008, p. 30).

As redes de comunicações eletrónicas são o ponto focal da sociedade de informação. A interligação existente entre sistemas operando continuamente e a utilização generalizada de aplicações comerciais de *software* e *hardware*, potenciaram o risco do efeito "dominó", em termos tecnológicos, que se poderá manifestar local ou globalmente

(Ferreira, 2008, p. 42). De facto, em todo este processo, a segurança raramente tem constituído uma prioridade. Segundo Santos (2008, p. 30), as preocupações têm-se centrado na disponibilidade de serviço (*business continuity*) e salvaguarda da informação (*backups*), no acesso físico às instalações e à ameaça interna (quadro de pessoal).

Dever-se-á ter sempre presente que os sistemas de informação e de comando e controlo são sistemas altamente complexos, constituídos por uma grande variedade de componentes, interligados e interdependentes, e cujas características intrínsecas proporcionam, em caso de ataque, um efeito de disrupção em cascata, com resultados imprevisíveis, mas de certo relevantes. A informatização das actividades e o uso da internet apresenta vantagens, mas também vulnerabilidades, que podem ser exploradas por todo o tipo de organizações, como é o caso das terroristas.

Segundo Joseph Nye Jr. (2002, p. 273), os "grupos terroristas poderiam espalhar o terror atacando os sistemas de informação que controlam a eletricidade dos hospitais, radares de controlo aéreo ou transações bancárias. Tais ataques poderiam ser perpetrados com fortes explosivos em locais de importantes computadores-servidores, mas poderiam igualmente ser executados transnacionalmente por *hackers* informáticos a dezenas de milhares de quilómetros de distância". Atualmente, a violência tem uma origem difusa, é imprevisível, assimétrica e global (Cardoso, 2007, p. 6) e quanto maior for a dependência diária da sociedade relativamente às TIC, maior será o risco e o dano social de um ciberataque (Bravo, 2010, p. 17).

Como defende Graça (2009, p. 113), com o qual concordamos, "o ciberterrorismo é, neste momento, uma das ameaças mais complexas que impende sobre o mundo ocidental. A singularidade da situação tem sobretudo a ver com o elevado grau de incapacidade de previsão dos serviços de informações quanto à ocorrência de ataques aos sistemas informáticos, da incerteza quantos aos efeitos produzidos e da real impossibilidade de resposta em tempo útil por parte das autoridades. O problema não reside na probabilidade de tais ataques vitimarem diretamente pessoas, mas sim de destruírem sistemas e subsistemas administrativos, financeiros e económicos - públicos e privados - que sustentam as atividades diárias dos países e respetivas populações".

A monitorização constante dos sistemas de informação e de comando e controlo deverá ser assegurada e garantida, como forma de minimizar as ameaças e riscos que recaem sobre eles. Normalmente, as medidas de segurança implementadas têm como objetivos comuns a confidencialidade, a integridade e a disponibilidade, sendo

fundamental para atingir esses objetivos a autenticação, a autorização, o controlo de acesso, a auditoria e a contabilização (Ferreira, 2008, p. 42).

A segurança e o bom funcionamento destes sistemas são colocados em causa por ameaças não convencionais, sendo absolutamente necessário agir em antecipação e preventivamente, no sentido de encontrar soluções que garantam a sua segurança e resiliência. Como a estanquicidade das ameaças foi quebrada há muito, a sua manifestação e impacto, mesmo que inicialmente focalizada num determinado sistema de uma empresa ou organização, poderá alastrar-se e ter repercussões noutras empresas ou organizações, fruto da crescente interdependência. Assim, o problema de uns poderá ser o problema de muitos, pelo que só com colaboração e cooperação entre os proprietários e gestores destes sistemas, e os organismos de segurança e defesa estatais, será possível o combate eficaz destas ameaças.

O grande desafio que se nos apresenta é o de conseguir implementar um funcionamento distribuído e orquestrado de todas as entidades envolvidas neste combate, de forma a ser possível proteger de forma cabal as IC (Amaral, 2008, p. 58).

É pois um facto assente que, cada vez mais, dependemos e nos apoiamos nas modernas TIC para o funcionamento dos vários sectores da nossa sociedade. A crescente quantidade de informação ligada em rede, bem como a complexidade dos sistemas de informação, torna-os extraordinariamente vulneráveis à ameaça ciberterrorista e, consequentemente também as IC e o normal funcionamento de um país.

Esta crescente importância e dependência exigem a tomada de medidas de segurança, à semelhança das já tomadas para proteger as IC portuguesas, sendo fundamental a definição de uma estratégia nacional que identifique objetivos, oriente esforços e enquadre a atuação das diferentes entidades envolvidas nesta luta, bem como outras medidas que privilegiem a cooperação e a complementaridade para que esta ameaça seja encarada e combatida de forma global.

c. Síntese conclusiva

A vivência humana é um sistema complexo, recheado de subsistemas que se interligam e interagem numa teia de relações de dependência contínua. Esta interdependência tem sido alavancada e potenciada pelas modernas tecnologias, que fazem hoje parte do dia-a-dia das populações e das quais dependemos para a realização de uma infindável quantidade de atividades, sem que muitas vezes nos apercebamos desse facto. Deste sistema de sistemas fazem parte alguns elementos que têm mais importância que

outros e que são catalogados pelos Estados como IC, cuja importância para a segurança e normal funcionamento da vida das sociedades determina a sua proteção.

Acontecimentos terroristas recentes contribuíram para a consciencialização dos Estados e organizações supranacionais, das vulnerabilidades destas estruturas e para os riscos e consequências catastróficas que a sua disrupção poderia acarretar. Foram já tomadas medidas de proteção, das quais se destacam as elencadas pela UE no seu PEPIC. Portugal, tendo como referência o programa europeu, tem já em desenvolvimento o seu próprio programa, o PNPIC, tendo sido identificadas e classificadas as ICN, e estando em curso o estudo e definição de medidas eficientes para o reforço da sua proteção. Como muitas das ICN são propriedade de privados é crucial a cooperação, coordenação e a partilha de responsabilidades e custos, no sentido de melhorar a implementação das necessárias medidas de segurança.

A informação sempre foi, e continua a ser, fundamental para o sucesso da tomada de decisão, sendo uma fonte de poder vital em qualquer organização. Os sistemas de informação e de comando e controlo, fruto do avanço tecnológico, baseiam-se e dependem das modernas TIC, e as caraterísticas destas, além de tornar os sistemas eficazes e eficientes, apresentam vulnerabilidades que podem ser exploradas até por organizações terroristas. Os ataques a estes sistemas têm um impacto disruptivo, provocando a propagação em cascata dos seus efeitos aos restantes sistemas a eles ligados, causando não só elevados prejuízos e perdas económicas, como colocando em causa a segurança e o bem-estar da população de um país, ou mesmo de países vizinhos.

Assim, confirma-se a **H2**, a interrupção de sistemas pode ter consequências muito negativas para um país, caso estas sejam disruptivas, de grande alcance e por um período de duração suficiente para causar danos de elevada monta, ficando respondida a **QD2:** "D**e** que forma a interrupção de sistemas pode ter como consequência o colapso, mesmo que parcial, de um país?"

3. Estratégia Nacional de Cibersegurança – Estudos de caso

a. As medidas de prevenção e proteção contra o ciberterrorismo

O terrorismo, como ameaça cada vez mais importante e efetiva, obrigou os Estados a criarem organismos, a organizarem as estruturas já existentes e a tomarem medidas específicas para o seu combate. A estrutura portuguesa de prevenção e combate ao terrorismo encontra-se plasmada no Apêndice 6 deste trabalho.

O ciberataque à Estónia levou a NATO a reagir e a desenvolver um conjunto de ferramentas, bem como a capacidade de ajudar os seus membros a defenderem-se contra futuros ataques. Assim, foi criado a *Cyber Defense Management Authority* (CDMA), em Bruxelas, de forma a centralizar as capacidades operacionais de defesa cibernéticas da Aliança, coordenando as respostas dos seus membros em caso de um ciberataque. De igual modo foi criado em Talin, na Estónia, o *Cooperative Cyber Defense Centre of Excellence* (CCD CoE) com a missão de desenvolver, a longo prazo, a doutrina e a estratégia de defesa cibernética da NATO (Hughes, 2009). O Conceito Estratégico da NATO de 2010 realça a necessidade de desenvolver a capacidade de prevenir, detetar, defender e recuperar de ciberataques. A 8 de junho de 2011 foi aprovada a *NATO Policy on Cyber Defense*, cujo principal foco consiste na proteção das suas comunicações e sistemas de informação. Esta política tem como objetivos a futura integração da ciberdefesa no *NATO Defense Planning Process* (NDPP) e o desenvolvimento de requisitos mínimos para as redes nacionais que estão ligados às redes da NATO. Os esforços de ciberdefesa da NATO baseiam-se nos princípios gerais da prevenção e resiliência e da não duplicação, prestando a NATO assistência coordenada se um ou mais aliados forem vítimas de um ciberataque (NATO, 2011).

A UE, igualmente consciente desta nova ameaça, adotou a Convenção sobre o Cibercrime a 23 de novembro de 2001, aprovada por Portugal a 15 de setembro de 2009, com o objetivo de criminalizar a prática de atos ilícitos relacionados com sistemas e dados informáticos (Assembleia da República, 2009b). Foi também criada a *European Network and Information Security Agency* (ENISA), que trabalha para as instituições da UE e EM, para prevenir, tratar e responder às questões de segurança cibernética da UE. Esta agência é um centro especializado em segurança de redes e da informação, cujo objetivo é estimular a cooperação entre os setores público e privado. As suas principais tarefas são: aconselhar a Comissão e os EM em matéria de segurança da informação e no seu relacionamento com a indústria para tratar problemas relacionados com a segurança de

hardware e *software*; recolher e analisar os dados sobre incidentes de segurança na Europa e riscos emergentes; fomentar métodos de gestão e avaliação de riscos e sensibilizar e cooperar com os diferentes intervenientes no domínio da segurança da informação (ENISA, 2012).

Portugal não dispõe nem de uma estratégia de cibersegurança, nem de entidades primariamente responsáveis pela coordenação de uma resposta concertada nesse domínio, sejam ao nível político, estratégico ou militar, formalmente mandatadas, do ponto de vista legal, para a exercer (Nunes, 2012). No entanto, existe uma rede de *Computer Security Incident Response Team* (CSIRT) a nível nacional, que pretende estabelecer um ambiente de cooperação e assistência mútua no tratamento de incidentes e na partilha de boas práticas de segurança. Esta rede, atualmente, é composta por 14 CSIRT[16] de vários sectores de atividade, tais como: telecomunicações, energético, bancário, académico e de defesa (FCCN, 2011).

Os serviços de resposta a incidentes de segurança informática têm sido apontados como essenciais na prevenção e reação a este tipo de fenómeno. Neste contexto, a Fundação para a Computação Científica Nacional (FCCN)[17], apresenta uma longa experiência a nível nacional e internacional, quer no tratamento e na coordenação da resposta a incidentes, quer na divulgação e outras formas de promoção do conceito CSIRT dentro do território nacional.

O CERT.PT tem funcionado como "o CERT nacional de facto, mas não de *jure*" (Nunes, 2012), tendo vindo a promover a criação de novas CSIRT, facilitando ações de formação e dando o apoio necessário ao seu estabelecimento.

A Secção de Investigação de Criminalidade Informática e de Telecomunicações da Policia Judiciária tem a competência nacional para a investigação da criminalidade informática e alguns dos crimes praticados com recurso a meios informáticos (FCCN, 2012).

Sendo o ciberterrorismo uma verdadeira nova ameaça, as FFAA deverão estar igualmente preparadas para lhe responder. Para isso, será necessário desenvolver capacidades defensivas e ofensivas, de forma a impedir que os sistemas de informação utilizados pelo país sejam paralisados, bem como impedir a interferência e neutralização

[16] Era este o número em 20 de fevereiro de 2012, podendo a identificação das várias CSIRT ser consultada em http://www.cert.pt/index.php/pt/rede-nacional-csirt/directorio .
[17] Através do seu serviço *Computer Emergency Response Team* (CERT) - o CERT.PT.

dos seus sistemas de armas, e poder atacar os sistemas do adversário (Santos, 2003, p. 227).

As FFAA não têm nenhum mandato para intervir neste domínio. No entanto, têm a responsabilidade de atuar contra ameaças externas, assim como quando as IC do país forem atacadas e este entrar em colapso, à semelhança da Estónia. Por esta razão, as FFAA deverão possuir a capacidade para defender o país deste tipo de ameaças. A acrescentar a esta situação está o facto de nos encontrarmos à beira de uma militarização do ciberespaço, com os EUA a criarem o USCIBERCOM, um comando com a mesma importância dos restantes comandos, e com uma série de outros países também com capacidades cibernéticas militares. Portugal, com as suas FFAA, ou acompanha este processo e procura estar a par da situação, ou então é ultrapassado e deixa de estar dentro do "circulo de confiança", deixando de ser considerado (Nunes, 2012).

Poderemos então afirmar, tal como defende o Dr. Alexandre Caldas (2011, p. 94), de que "a crescente importância das TIC em todas as esferas da sociedade, e naturalmente na Segurança e Defesa Nacional, a questão da "Cibersegurança" assumiu uma dimensão estratégica. Torna-se, assim, imperativa a definição de uma Estratégia Nacional de Cibersegurança".

b. As Estratégias de Cibersegurança dos EUA, Reino Unido, França e Alemanha

O desenvolvimento e implementação de uma ENC é uma necessidade essencial e premente na atualidade, em que cada vez mais as ciberameaças ganham visibilidade e importância para a segurança nacional, tendo já vários países definido a sua própria estratégia.

Assim, propomos fazer de seguida a análise das estratégias de alguns países da NATO e UE, cuja importância e influência na tomada de decisão sobre o rumo destas organizações supranacionais, das quais Portugal faz parte, é em nossa opinião determinante, pelo que deverão ser consideradas na criação da nossa estratégia.

(1) EUA

De acordo com Eneken Tikk (2011, pp. 154-235), a visão americana para a sua estratégia de cibersegurança é de proteger os sistemas de informação das infraestruturas críticas e, assim, ajudar a proteger as pessoas, a economia e a segurança nacional. Para o conseguir, terão de ser atingidos os seguintes objetivos: prevenir ciberataques contra as IC americanas, reduzir a vulnerabilidade nacional contra os

ciberataques e minimizar os danos e o tempo de recuperação no caso de ocorrência de ciberataques.

A estratégia americana, datada de fevereiro de 2003, articula-se e desenvolve-se segundo cinco prioridades: estabelecer um sistema nacional de resposta para a segurança do ciberespaço; criar um programa nacional de redução das vulnerabilidades e ameaças; desenvolver um programa nacional de treino e consciencialização para a segurança do ciberespaço; garantir a segurança do ciberespaço do Governo e por último, fomentar a cooperação a nível nacional e internacional.

Para o desenvolvimento destas prioridades está subjacente a implementação de um vasto conjunto de medidas que a seguir se apresentam:

- Estabelecer uma arquitetura público-privada para responder a nível nacional a ciberataques;
- Fornecer análise de ciberataques e avaliação de vulnerabilidades para o desenvolvimento de táticas e estratégias;
- Incentivar o setor privado a partilhar uma visão sinóptica do estado de saúde do ciberespaço;
- Expandir a Rede de Informação e Aviso Cibernética de apoio ao papel do *Department of Homeland Security* (DHS), que coordena a gestão de crises para a segurança do ciberespaço;
- Melhorar a gestão nacional de incidentes e coordenar a participação voluntária público-privada no desenvolvimento de planos nacionais de contingência e continuidade;
- Melhorar a aplicação da legislação de prevenção e repressão de ciberataques;
- Criar um processo de avaliação das vulnerabilidades nacionais, compreender as interdependências das infraestruturas e melhorar a segurança física dos sistemas cibernéticos e de telecomunicações;
- Promover um programa nacional de consciencialização abrangente para que as empresas e a população em geral, garantam a segurança da sua parte do ciberespaço, bem como promover programas de formação e treino adequados;
- Avaliar continuamente as ameaças e vulnerabilidades dos sistemas cibernéticos do Governo, autenticar os seus utilizadores autorizados, garantir a segurança das redes sem fio federais e melhorar a segurança nas aquisições e no *outsourcing* do Governo;

- Melhorar a capacidade de atribuição do ataque e da resposta e promover a criação de redes nacionais e internacionais de vigilância e alerta para prevenir e detetar ciberataques;
- Incentivar outras nações a aderir à Convenção do Conselho da Europa sobre o cibercrime, ou assegurar que as suas leis e procedimentos são, pelo menos, abrangentes.

(2) Reino Unido

A estratégia de cibersegurança do Reino Unido foi aprovada em junho de 2009, pretendendo que os cidadãos, as empresas e o Governo possam desfrutar dos benefícios e das oportunidades de um ciberespaço seguro e resiliente e que, trabalhando em conjunto, seja possível compreender e enfrentar os riscos, reduzindo os benefícios dos terroristas e criminosos.

Apresenta como objetivos: a redução do risco do uso do ciberespaço; a exploração das suas oportunidades e por último, o melhoramento dos conhecimentos, das capacidades e da tomada de decisão. Estes objetivos serão alcançados segundo as seguintes linhas de ação: o estabelecimento de um programa intragovernamental, que aborde as áreas prioritárias para a cibersegurança dos objetivos estratégicos; trabalhar de perto com o sector público, com a indústria, como os grupos de liberdades civis e com os parceiros internacionais, e finalmente, criar o *Office of Cyber Security* (OCS) e o *Cyber Security Operations Centre* (CSOC).

As linhas de ação referidas necessitam da implementação das seguintes medidas:

- Melhorar a preparação e proteção contra ciberataques em todos os setores, estabelecendo medidas de mitigação apropriadas, redundantes, resilientes e permitindo a continuidade de negócios para o Governo e outros setores críticos;
- Identificar lacunas na doutrina existente, na política, nas estruturas legais e regulamentares (tanto nacionais como internacionais) e, se necessário, tomar medidas para corrigi-las, desenvolvendo o quadro jurídico para a cibersegurança;
- Aumentar a sensibilização para a cibersegurança e identificar e incutir mudanças de comportamento e cultura de trabalho;
- Garantir o crescimento das capacidades e conhecimentos necessários, pelo Governo e pela indústria, no campo da cibersegurança e desenvolver capacidades técnicas e de pesquisa;

- Impulsionar o desenvolvimento de um quadro coerente para a compreensão e comunicação dos riscos, oportunidades e impactos associados ao ciberespaço;
- Promover a participação público-privada no desenvolvimento de planos e na implementação de medidas de cibersegurança. Incentivar a partilha de informação, e apoiar e aconselhar em questões relacionadas com a cibersegurança;
- Fornecer, através do OCS, liderança estratégica e coerência dentro do Governo para as questões de cibersegurança;
- Monitorizar, através do CSOC, o ciberespaço, analisar tendências e coordenar a resposta técnica a ciberataques, e proporcionar aconselhamento e informação sobre os riscos para os negócios e para o público em geral.

A estratégia demonstra que o Reino Unido reconhece a sua crescente dependência do ciberespaço, bem como a importância e os desafios que a sua segurança acarreta (Tikk, 2011, pp. 84-99).

(3) França

A França tomou recentemente medidas no sentido de se proteger em matéria de cibersegurança, atualizando em fevereiro do ano transato a sua estratégia. Apresenta como visão, garantir a cibersegurança dos seus compatriotas, dos seus negócios e da Nação.

Para alcançar tal desiderato pretende: ser uma potência mundial em Ciberdefesa; garantir a liberdade de decisão através da proteção de informações soberanas; reforçar a cibersegurança das ICN e perceber e garantir a segurança do ciberespaço. Estes objetivos serão alcançados através de: deteção e combate de ataques; da antecipação e análise do ambiente, para tomar decisões informadas e adaptadas; alerta e apoio às potenciais vítimas; crescimento e solidificação das capacidades científicas, técnicas, industriais e humanas e da proteção dos sistemas de informação do Estado e dos operadores das IC. Será igualmente necessário: a adaptação das leis tendo em conta a evolução tecnológica; o desenvolvimento da colaboração internacional na proteção dos sistemas de informação na luta contra o cibercrime e na defesa dos seus sistemas de informação e, por último, a educação e persuasão do povo francês para que compreendam a importância da segurança dos sistemas de informação.

A operacionalização de toda a estratégia será feita implementado as seguintes medidas:

- Acompanhar as últimas novidades no mundo da tecnologia;

- Desenvolver as capacidades para a deteção de ataques contra os sistemas de informação;
- Criar uma sala de operações pela *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI) para gerir e coordenar as informações colhidas pelos dispositivos de vigilância ou transmitidas por parceiros, verificar o estado das redes nacionais em tempo real e gerir crises;
- Assegurar, através da ANSSI, o funcionamento da autoridade nacional para a defesa dos sistemas de informação;
- Criar, com parceiros industriais, um centro de pesquisa para a realização da investigação científica (em criptologia, na análise dos atacantes, dos métodos utilizados e de *softwares* mal intencionados, no desenvolvimento de *software* seguro gratuito, etc), avaliações e treino;
- Redefinir a estratégia de produtos e de componentes de segurança relativos às informações classificadas;
- Implementar as redes ministeriais de sistemas de autenticação (cartões inteligentes) e utilização das redes seguras interministeriais de internet, videoconferência e telefónica;
- Transpor as diretivas europeias para o direito francês;
- Estabelecer uma ampla gama de parcerias, incentivando a partilha de dados essenciais, nomeadamente sobre vulnerabilidades ou deficiências em produtos e serviços;
- Partilhar informações com os parceiros sobre a luta contra o cibercrime, estabelecendo, com um círculo restrito de aliados, intercâmbios operacionais aprofundados;
- Fornecer apoio específico, através da ANSSI, aos decisores das diversas áreas, ajudando-os a expandir as medidas e a tomar as decisões necessárias para garantir a segurança dos sistemas de informação, além de desenvolver uma comunicação abrangente e adequada dirigida ao público e às empresas.

O Governo francês realça a importância que confere ao combate das ciberameaças, fazendo uma analogia entre este e o combate travado entre os gregos e os persas na célebre batalha das Termópilas (Tikk, 2011, pp. 76-82).

(4) Alemanha

Segundo Eneken Tikk (2011, pp. 40-52), em julho de 2005 a Alemanha definiu a sua estratégia de cibersegurança com a finalidade de fortalecer a defesa das suas

infraestruturas de informação contra as ameaças globais, estabelecendo como objetivos estratégicos: proteger de forma adequada essas infraestruturas; responder eficazmente a incidentes de segurança relacionados com TIC e melhorar a competência alemã em cibersegurança e no estabelecimento de padrões internacionais.

As linhas de ação a seguir são: aumentar a conscientização dos riscos relacionados com o uso de TIC; usar produtos e sistemas de TIC seguros; respeitar o sigilo e implementar salvaguardas, bem como a criação de condições e diretrizes enquadrantes e estratégias coordenadas de segurança. É igualmente fundamental a identificação, registo, avaliação, alerta e resposta a ciberataques, melhorando a competência em cibersegurança, fomentando a educação e a formação profissional nesta área. A investigação e o desenvolvimento, a par com a cooperação internacional são prioridades basilares da estratégia.

Associadas a estas prioridades e linhas de ação estão as seguintes medidas:

- Implementar iniciativas de sensibilização abrangentes, dirigidas a todos os níveis da gestão empresarial e da administração pública, aos trabalhadores comuns e aos utilizadores individuais de computadores;
- Apoiar o uso de produtos e sistemas de TIC confiáveis, sobretudo na administração federal, ampliando e melhorando, através do *Bundesamt für Sicherheit in der Informationstechnik* (Serviço Federal de Segurança da Informação-BSI) a capacidade de examinar e avaliar produtos e sistemas de TIC, sob os aspetos de segurança e emissão de certificados;
- Efetuar recomendações e orientações técnicas, através do BSI, para a utilização destes produtos e publicar a lista de produtos certificados;
- Promover o desenvolvimento e o fabrico de produtos alemães de criptografia e usar a criptografia e aplicações de segurança nas comunicações do Governo;
- Fornecer recomendações e orientações sobre segurança de TIC a todas as áreas da sociedade e, especificamente, àqueles ramos da economia com requisitos especiais de segurança;
- Reforçar a cooperação nacional e internacional, de forma a defender os interesses de segurança alemães aquando da formulação de orientações, diretrizes e outros instrumentos jurídicos;

- Desenvolver um centro nacional de resposta crises de TIC e, através deste, comandar, controlar, analisar e fornecer avaliações fiáveis da atual situação de segurança alemã, e cooperar com outros centros existentes, no controle de determinado incidente ou crise;
- Criar um sistema de alerta, para informar de forma rápida e abrangente todos os potencialmente afetados, sobre ameaças e ataques iminentes contra infraestruturas de informação;
- Implementar nos currículos dos cursos e na formação profissional, matérias relacionadas com a cibersegurança. Expandir e melhorar os serviços de informação dos cidadãos, escolas, universidades, empresas privadas e administração pública, aumentando a consciência sobre as questões de cibersegurança na sociedade como um todo;
- Apoiar a investigação científica alemã, defendendo a participação de empresas alemãs em pesquisas e programas de tecnologia internacional (nomeadamente ao nível da UE) e, intensificar a cooperação entre a indústria e a investigação realizada nas universidades;
- Defender os interesses de segurança alemães no estabelecimento de normas internacionais de proteção de estruturas de informação;
- Reforçar a nível nacional, interministerial e interdisciplinar, a cooperação na elaboração de normas e leis.

c. Análise e ilações para uma Estratégia Nacional de Cibersegurança

Sendo um facto que a realidade portuguesa é semelhante à de outros países desenvolvidos, no que respeita à crescente importância e dependência dos sistemas de informação e das TIC que os compõem, nos diferentes sectores da sociedade, tal situação implica a necessidade de serem tomadas medidas que garantam o funcionamento e utilização segura destes sistemas e tecnologias pelos seus utilizadores.

A segurança do ciberespaço é indispensável, devendo ser uma preocupação transversal à sociedade, cabendo ao Estado liderar o processo de adoção de medidas para a atingir. Nesta ordem de ideias, faz parte do Plano Global Estratégico de Racionalização e Redução de Custos nas TIC na Administração Pública, aprovado pela Resolução de Conselho de Ministros n.º 12/2012, de 7 de Fevereiro, a definição e implementação de uma Estratégia Nacional de Segurança da Informação (ENSI)[18]. Esta estratégia incluirá um conjunto objetivo de vetores fundamentais para uma melhor proteção da informação

[18] Medida nº 4 do referido documento.

relevante para o Estado e para a sociedade, nomeadamente: a criação, instalação e operacionalização de um Centro Nacional de Cibersegurança (CNC); o aprofundamento e melhoria das condições de operação do Sistema de Certificação Eletrónica do Estado (SCEE); a criação e certificação de uma solução de criptografia forte de origem nacional e por último a revisão do quadro legal para a segurança das matérias classificadas, substituindo os regulamentos SEGNAC atualmente em vigor. O desenvolvimento desta medida será coordenado pelo Gabinete Nacional de Segurança (GNS) (GPTIC, 2011).

A ENSI será o "chapéu" que enquadrará e orientará todos os intervenientes da sociedade (Estado, empresas e cidadãos), para uma melhor e adequada proteção da informação e dos sistemas de informação. Em nossa opinião está incompleta, devendo ser definida e implementada uma ENC, que constituirá o quinto vetor da ENSI, que enquadre e oriente a proteção do ciberespaço português. Desta forma, a criação, instalação e operacionalização do CNC, deve estar em linha com as orientações definidas na ENC.

Tendo como base de partida os exemplos apresentados e a realidade nacional, e como resultado da sua análise, verificamos os pontos comuns e de convergência das várias estratégias, identificando de seguida os aspetos mais relevantes e que, em nossa opinião, deverão constar de uma futura ENC.

Assim, todas as estratégias contemplam a existência de um organismo responsável por monitorizar e avaliar o ambiente cibernético do país, alertando para a existência de possíveis ameaças, recomendando ações de proteção e combate e coordenando as respostas das diversas entidades com responsabilidades nesta área. É importante referir que, a materialização das capacidades nacionais em matérias de cibersegurança, que à partida estarão assentes no CNC, não se podem confundir com a "simples" criação de um CSIRT de âmbito nacional. Devem acima de tudo, estar vocacionadas para a proteção da informação relevante do Estado, das empresas e dos cidadãos, de modo a que em caso de materialização das ameaças, os danos resultantes possam ser absorvidos na sua grande maioria pela robusta proteção dos sistemas de informação. Desta forma, a capacidade de resposta a incidentes ficará para fazer face a ataques mais sofisticados, que as medidas de proteção "*standard*", não foram capazes de reter.

Efetuar uma avaliação rigorosa da situação, identificando lacunas e vulnerabilidades, estudando quais as medidas adequadas a implementar e recomendando ações que tornem a proteção das IC mais eficaz e eficiente. Incentivar a partilha de informação e promover ou reforçar a cooperação pública e privada quer ao nível nacional quer internacional.

Criar ou adaptar um quadro normativo e legislativo que regule a atuação no ciberespaço, fomentar campanhas de sensibilização, apostando na formação e em projetos de investigação relacionados com a segurança das TIC.

Dada a caraterística sistémica desta realidade, o nível de segurança global é dado pelo nível mais baixo dos constituintes do sistema. Daqui resulta que o esforço de incrementar a segurança num determinado setor, poderá ser infrutífero se não for acompanhado por outros setores aos quais está ligado. Esta realidade é aplicável não só a nível nacional, como também a nível internacional. Assim, é fundamental que o Estado procure envolver todos os setores e entidades relevantes na elaboração da ENC, como forma de garantir uma abordagem holística, consensual e um entendimento alargado, que possibilite a sua eficácia e eficiência.

d. Síntese conclusiva

Os novos desafios de segurança e defesa que se colocam atualmente aos países são relevantes, complexos, diversos e difíceis de prever e responder. O fenómeno da globalização está intrinsecamente ligado ao progresso tecnológico, nomeadamente no que respeita às TIC. Estas são ubíquas, tendo uma importância central em todos os setores da nossa sociedade. A crescente importância e dependência das TIC elegem-nas como alvos extremamente importantes, e obrigam os Estados a tomar medidas para a sua proteção e defesa. As consequências de um ataque bem-sucedido podem ser muito gravosas, podendo originar um fenómeno disruptivo em cascata de dimensões imprevisíveis.

As caraterísticas das TIC globalizam todas as atividades das sociedades e também as ameaças, passando o ciberterrorismo a constituir-se como uma nova e bem real ameaça. Uma ameaça global exige uma resposta igualmente global, multissectorial, internacionalmente integrada, agindo de preferência em antecipação.

Tendo consciência dos factos anteriormente referidos, organizações supranacionais como a NATO e a UE tomaram já algumas medidas para proteger os seus membros e os próprios países têm vindo, progressivamente, a criar estruturas, organizações e procedimentos para aumentar a sua proteção e resiliência em caso de ataque. Teremos de ter sempre bem presente que, num sistema em rede como aquele que estamos a tratar, a segurança total do sistema resulta diretamente do nível de segurança do elo mais fraco.

Portugal tem também já algumas entidades com responsabilidades em matéria de cibersegurança e alguns procedimentos em vigor, faltando, no entanto, entre outras coisas, uma ENC que oriente e coordene esforços para proteger os sistemas de informação

nacionais e responder eficazmente contra ciberataques. Muito ainda existe a criar e a melhorar em matéria de cibersegurança, sendo que a definição e implementação desta estratégia é de capital importância e constituirá as fundações onde será erigida a estrutura de cibersegurança nacional.

Desta forma, confirma-se a **H3**, Portugal têm consciência do impacto deste tipo de ataque e deve desenvolver estruturas e sistemas de prevenção e proteção que privilegiem a complementaridade e colaboração entre os diferentes agentes envolvidos neste combate, ficando respondida a **QD3**: "Quais os principais aspetos que deverão constar numa Estratégia Nacional de prevenção e combate ao ciberterrorismo?"

Conclusões e recomendações

a. Conclusões

Atualmente, o terrorismo tem uma presença ubíqua no dia-a-dia das populações em todo o mundo, influenciando o seu modo de vida. Os modernos meios de comunicação social têm mediatizado estes atos terroristas, através de imagens brutais e em tempo real, consciencializando as pessoas da ameaça eminente de ataques a qualquer momento e em qualquer lugar.

A forma de atuação dos terroristas tem vindo a sofrer alterações ao longo dos tempos, estando diretamente relacionada com a evolução tecnológica dos meios ao seu dispor. É neste contexto que o ciberterrorismo ganha relevo, dada a importância e a dependência que hoje temos dos sistemas de informação.

A globalização expandiu o terrorismo, deixando este de ser local ou regional e passando a ser transnacional.

Nesta ordem de ideias, propusemo-nos a responder à Questão Central, que orienta o nosso trabalho: "Que postura deverá Portugal adotar face à ameaça ciberterrorista com vista à interrupção de sistemas de informação?"

Para responder a esta questão identificamos três hipóteses de trabalho que procurámos testar ao longo do presente estudo.

No primeiro capítulo estudou-se a origem do terrorismo, concluíndo que este é bastante antigo e que foi acompanhando a evolução da humanidade, adaptando-se e, inclusivamente, incorporando os fatores marcantes dessa mesma evolução. Analisado nas diferentes épocas, várias são as interpretações e definições encontradas, que refletem as distintas visões, interesses e convicções dos atores envolvidos. No entanto, existem algumas caraterísticas comuns como a imprevisibilidade, a enorme e indiscriminada violência empregue, os objetivos políticos, religiosos ou ideológicos, sendo o alvo preferencial a população.

A evolução dos sistemas de informação leva a que estes ocupem nas sociedades modernas um papel central na vida da maioria das pessoas, das empresas e dos Estados, ocupando a internet um lugar de destaque. Atualmente, todos os principais sistemas de um país, quer sejam económicos, financeiros, de saúde, de comunicações, de transportes, de produção e distribuição de energia e água, de segurança ou defesa, entre outros, são geridos, ou dependem de alguma forma, de sistemas informáticos.

Inserido neste ambiente, onde os sistemas de informação e de comando e controlo dominam, cada vez mais, o dia-a-dia de uma nação, importa realçar a dependência que deles estamos sujeitos, surgindo assim o ciberterrorismo como uma ameaça, cuja capacidade disruptiva dos seus ataques coloca em causa a segurança nacional e internacional.

O ciberterrorismo constitui-se como uma ameaça cada vez mais real, apesar dos efeitos dos seus ataques nem sempre serem percetíveis e diretamente relacionáveis com ele próprio, pois este pode ser usado como a principal forma de ataque, como aconteceu no caso da Estónia, ou ser utilizado em conjugação com os métodos tradicionais, como por exemplo na obtenção de informações, comunicação e organização de ataques, de forma a aumentar a eficiência e eficácia destes.

Da análise efetuada concluímos que o ciberterrorismo representa uma alteração na estratégia de atuação dos grupos terroristas, pois, apesar dos objetivos destes grupos se manterem, os meios ao seu dispor e a forma de os utilizar evoluíram, alterando significativamente a sua forma de atuação.

Os ataques terroristas, visando a interrupção de sistemas, independentemente do método utilizado, ganharão preponderância e as IC dos países estão agora em risco devendo o ciberespaço passar a ser considerado como uma nova e importante componente.

Desta forma, confirmamos a primeira hipótese levantada, de que o ciberterrorismo é uma adequação face ao avanço tecnológico presente na vida das sociedades modernas, por parte dos grupos terroristas e configura uma mudança na sua estratégia de atuação.

No segundo capítulo analisou-se o fenómeno da interrupção de sistemas, evidenciando a importância e o impacto desta na vida das populações e no funcionamento dos Estados, realçando o papel fundamental dos sistemas de informação e de comando e controlo.

A sociedade é um sistema complexo, repleto de subsistemas que se interligam e interagem numa teia de relações de dependência contínua. Deste sistema de sistemas sobressaem alguns que são considerados, pelos Estados, como IC, de elevada importância para a segurança e normal funcionamento da vida das sociedades.

Como resultado da constatação das vulnerabilidades destas infraestruturas, dos riscos que correm e das consequências catastróficas que a sua disrupção poderia acarretar, os Estados tomaram medidas para a sua proteção. Assim, a UE definiu um programa de proteção das ICE, denominado de PEPIC e Portugal, tendo como referência este mesmo programa, tem já em desenvolvimento o seu PNPIC. Até ao momento, foram já

identificadas e classificadas as ICN, estando em curso o estudo e definição de medidas eficientes para o reforço da sua proteção.

As modernas TIC apresentam vulnerabilidades, muitas das vezes aproveitadas por organizações mal-intencionadas como as terroristas. Os ataques aos sistemas de informação e de comando e controlo têm um impacto disruptivo, provocando a propagação em cascata dos seus efeitos aos restantes sistemas a eles ligados, causando não só elevados prejuízos e perdas económicas, como colocando em causa a segurança e o bem-estar da população de um país, ou mesmo de países vizinhos.

Confirma-se assim a segunda hipótese formulada, de que a interrupção de sistemas pode ter consequências muito negativas para um país, caso estas sejam disruptivas, de grande alcance e por um período de duração suficiente para causar danos de elevada monta.

No terceiro capítulo efetuou-se a análise do sistema e estrutura de prevenção e combate ao ciberterrorismo existente em Portugal, bem como das estratégias de cibersegurança dos EUA, Reino Unido, França e Alemanha, identificando quais os aspetos que deverão constar na ENC.

As TIC globalizaram não só as atividades das sociedades, como também as ameaças que sobre elas pairam. Uma ameaça global exige uma resposta igualmente global, multissectorial, internacionalmente integrada, agindo de preferência em antecipação. Procurando dar uma resposta o mais abrangente possível, organizações como a NATO e a UE tomaram já algumas medidas para proteger os seus membros, tendo os próprios países individualmente vindo progressivamente a criar estruturas, organizações e procedimentos para aumentar a sua proteção e resiliência em caso de ataque. A segurança de um sistema em rede é igual ao nível de segurança do elo mais fraco desse sistema.

Portugal não dispõe de entidades primariamente responsáveis pela coordenação de uma resposta concertada no domínio da cibersegurança. Existe uma rede de 14 CSIRT a nível nacional, cada um responsável pela segurança da sua rede, e que procuram estabelecer um ambiente de cooperação e assistência mútua no tratamento de incidentes e na partilha de boas práticas de segurança. Esta rede abarca vários sectores de atividade, tais como, telecomunicações, energético, bancário, académico e de defesa.

A Secção de Investigação de Criminalidade Informática e de Telecomunicações da Policia Judiciária tem a competência nacional para a investigação da criminalidade informática e alguns dos crimes praticados com recurso a meios informáticos.

As FFAA contribuem para a cibersegurança nacional através do seu próprio CSIRT, o CC-CRISI, que funciona no EMGFA. Sendo o ciberterrorismo uma ameaça real, que poderá causar o colapso de algumas das IC do país, à semelhança do sucedido na Estónia, as FFAA deverão desenvolver capacidades de forma a estarem preparadas para contribuir para o seu combate.

Para que Portugal possa vir a ter um sistema de segurança realmente eficaz nesta área, existem ainda vários aspetos que necessitam de ser melhorados, entre os quais podemos destacar a criação de uma ENC, que oriente e coordene esforços para proteger os sistemas de informação nacionais e responder eficazmente contra ciberataques. A definição e implementação desta estratégia é de capital importância e constituirá as fundações onde será erigida a estrutura de cibersegurança nacional.

Desta forma, confirma-se a terceira hipótese formulada, de que Portugal têm consciência do impacto deste tipo de ataque, e deve desenvolver estruturas e sistemas de prevenção e proteção que privilegiem a complementaridade e colaboração entre os diferentes agentes envolvidos neste combate.

Relativamente à questão central formulada, onde se questiona que postura deverá Portugal adotar face à ameaça ciberterrorista com vista à interrupção de sistemas de informação, conclui-se que, Portugal deverá:

- Criar e implementar uma estratégia de cibersegurança que defina claramente os objetivos estratégicos, as linhas de ação a serem seguidas, que oriente e coordene a atuação de todos os intervenientes nesta área e que defina as suas competências.
- Criar uma entidade (CNC) que mantenha a *situation awareness* do ciberespaço português, difunda recomendações, enquadre e coordene a atuação dos organismos já existentes que se dedicam à cibersegurança e ao combate dos ciberataques.
- Fazer uma análise pormenorizada da realidade portuguesa, identificando as vulnerabilidades e adotando medidas de prevenção e proteção abrangentes, que incluam todos os atores nacionais, públicos e privados, devendo ter presente que o combate ao ciberterrorismo só é possível através da cooperação nacional e internacional.

b. Recomendações

Procurando contribuir para uma futura ENC, entendemos que esta deverá ter como finalidade o aumento da segurança e resiliência dos sistemas de informação nacionais, tendo como objetivos estratégicos a proteção desses sistemas e a resposta eficaz contra

ciberataques. A estratégia deverá assentar em cinco pilares: a proteção dos sistemas de informação das IC; a deteção, alerta e resposta a ciberataques; a adaptação e criação de leis e normas reguladoras; a educação e formação e por fim, a cooperação nacional e internacional.

De forma a concretizar estes pilares de atuação, e da análise efetuada, seria importante implementar as seguintes medidas:

- Identificar vulnerabilidades e implementar medidas de proteção, redundantes, que garantam a resiliência e a continuidade de negócio das IC, públicas e privadas;
- Incentivar o setor público e privado a tomar medidas adequadas para proteger os seus sistemas de informação;
- Que o CNC, cuja criação, instalação e operacionalização está em curso, de uma forma geral, efetue o acompanhamento e avaliação da situação cibernética nacional, que emane alertas e recomendações à rede de CSIRT e que, seja responsável pela gestão, partilha de informação e coordenação de respostas a ciberataques por parte dos CSIRT. No entanto, que não se cinja às responsabilidades típicas de um CSIRT nacional, mas que tenha uma missão e enquadramento mais abrangente, nomeadamente:
  - Constituir-se como o ponto de contacto nacional para as matérias relacionadas com a cibersegurança, sendo a entidade responsável por fomentar e promover a cooperação nacional e internacional e representando Portugal nos fóruns internacionais;
  - Constituir-se como o ponto central de receção de informações sobre ciberataques, de modo a poder ser criada uma base de dados de histórico de incidentes, para memória futura e manter atualizada a visão global das ameaças em coordenação com os Serviços de Informações;
  - Constituir-se como a entidade coordenadora e garantir a articulação entre as entidades responsáveis pela resposta a incidentes, pela investigação e combate ao ciberterrorismo e cibercrime;
  - Constituir-se como a entidade coordenadora do desenvolvimento de doutrina, fornecendo apoio e aconselhamento em matérias de cibersegurança;
  - Criar mecanismos de coordenação para a recolha de informações sobre ameaças identificadas ou suspeitas;

  - Promover a ampliação da rede nacional de CSIRT já existente, definindo os requisitos mínimos das suas capacidades, bem como as normas de atuação;
  - Contribuir para a limitação e minimização do impacto dos ciberataques sobre os interesses nacionais;
  - Contribuir para a avaliação das interdependências e vulnerabilidades das IC de informação;
  - Contribuir para a redução das vulnerabilidades das IC nacionais face aos ciberataques;
  - Contribuir para a promoção da formação e sensibilização em cibersegurança;
- Criar um CSIRT governamental, responsável pela proteção e resposta a incidentes da rede da administração pública;
- Adaptar a legislação internacional à nossa realidade;
- Incentivar a partilha de informação em matérias de cibersegurança;
- Definir com clareza as entidades responsáveis pela investigação e combate ao ciberterrorismo e cibercrime;
- Definir e fiscalizar, através da Autoridade Nacional de Comunicações (ANACOM), a implementação de regras e medidas de segurança pelas operadoras de comunicações eletrónicas, para que garantam um nível mínimo de segurança das comunicações;
- Efetuar, através do GNS, a revisão e atualização das instruções para a segurança nacional, salvaguarda e defesa das matérias classificadas (SEGNAC), criar normas a aplicar pela administração pública e pelas entidades que com ela se relacionam, estabelecer a certificação de produtos e fazer auditorias;
- Promover campanhas de sensibilização abrangentes, alertando para os riscos, perigos e para o contributo que cada um pode dar para o aumento da cibersegurança nacional;
- Impulsionar a formação de técnicos especializados em matérias relacionadas com a cibersegurança, bem como do cidadão comum;
- Fomentar e apoiar o desenvolvimento de projetos nas universidades no domínio da segurança dos sistemas de informação.

Assim, julgamos que as recomendações propostas poderão auxiliar a criação da ENC, tarefa de elevada responsabilidade e importância para a segurança nacional, que requer estudos e debates aprofundados, e a participação alargada das entidades dos vários setores que têm experiência e conhecimento nesta área, de forma a obter uma visão holística do problema.

Bibliografia[19]

Abrial, S, 2011. NATO Builds Its Cyberdefenses. *The New York Times*

Academia das Ciências de Lisboa, 2012. *Ciberespaço: Espaço Virtual, Mediático e Global.* Academia das Ciências de Lisboa, 25 de janeiro de 2012. Lisboa

Alberto, C, 2011. Infra-Estruturas Críticas Nacionais: Protecção, Prevenção e Resposta a Ameaças. *Segurança e Defesa*, janeiro-março, pp. 14-22

Amara, JB, 2011. Nova vaga de ataques informáticos aos sites do Parlamento, PSP e Finanças. *Jornal Público*

Amaral, PC, 2008. A Importância da Gestão do Conhecimento na Resposta às Novas Ameaças à Segurança. *Planeamento Civil de Emergência, nº20*, pp. 52-59

Assembleia da República, 2003. *Lei de combate ao terrorismo* (Lei n.º 52/2003 de 22 de Agosto), Lisboa: Diário da República

Assembleia da República, 2007. *Lei Orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa (SIED) e do Serviço de Informações de Segurança (SIS)* (Lei n.º 9/2007 de 19 de fevereiro), Lisboa: Diário da República

Assembleia da República, 2008a. *Lei Orgânica da polícia Judiciária* (Lei n.º 37/2008 de 06 agosto), Lisboa: Diário da República

Assembleia da República República, 2008b. *Lei de Organização da Investigação Criminal* (Lei n.º 49/2008 de 27 de agosto), Lisboa: Diário da República

Assembleia da República, 2008c. *Lei da Segurança Interna* (Lei n.º 53/2008 de 29 de agosto), Lisboa: Diário da República

Assembleia da República, 2009a. *Lei Orgânica de Bases da Organização das Forças Armadas* (Lei Orgânica n.º 1-A/2009 de 07 de julho), Lisboa: Diário da República

[19] Na realização do trabalho foi utilizada a ferramenta de referenciação automática incorporada no Microsoft Word, tendo sido utilizado o estilo "Harvard – Anglia", tal como previsto na Norma de Execução Permanente nº 218 do Instituto de Estudos Superiores Militares.

Assembleia da República, 2009b. *Aprova a Convenção sobre o Cibercrime, adoptada em Budapeste em 23 de Novembro de 2001* (Resolução da Assembleia da República n.º 88/2009 de 15 de setembro), Lisboa: Diário da República

Assembleia da República, 2009c. *Lei do Cibercrime* (Lei n.º 109/2009 de 15 de setembro), Lisboa: Diário da República

Assembleia da República, 2011. *Procedimentos de identificação e de protecção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos sectores da energia e transportes* (Decreto-Lei n.º 62/2011 de 9 de maio), Lisboa: Diário da República

Baker, S et al., 2010. *Sob fogo cruzado: Infraestrutura crítica na era da guerra cibernética,* São Paulo: McAfee

Batista, G et al., s.d. C*iberterrorismo: A Nova Forma de Crime do Sec. XXI, Como Combatê-la.* [Em linha] Disponível em: http://www.academiamilitar.pt/proelium-n.o-1.html [Consult. 31 outubro 2011]

Bravo, R, 2010. *Do Espectro de Conflitualidade nas Redes de Informação: por uma Reconstrução Conceptual do Terrorismo no Ciberespaço.* [Em linha] Disponível em: http://ual-pt.academia.edu/RogerioBravo/Papers/713926/Do_espectro_de_conflitualidade_nas_redes_de_informacao_por_uma_reconstrucao_conceptual_do_terrorismo_no_ciberespaco [Consult. 2 fevereiro 2012]

Bravo, R, 2012. *Terrorismo: A Interrupção de Sistemas.* Entrevistado por Alexandre Varino. Direção Nacional da Polícia Judiciária, Lisboa, 30 jan 2012

Brundidge, G, 2011. *Partnerships in Cyber Security.* IDN, 14 dezembro 2011. Lisboa

Caldas, A, 2011. Uma Estratégia Nacional de Cibersegurança (ENC). *Segurança e Defesa,* janeiro-março, pp. 94-98

Cardoso, L S, 2007. Os Ciber-ataques e a Soberania Nacional. *Planeamento Civil de Emergência,* nº19, pp. 4-8

Center for Strategic and International Studies, 2006. *Significant Cyber Incidents Since 2006.* [Em linha] Disponível em: http://csis.org/publication/cyber-events-2006 [Consult. 5 janeiro 2012]

CIA, 2011. *The World Factbook.* [Em linha] Disponível em: https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html [Consult. 30 dezembro 2011]

Conselho da União Europeia, 2001a. P*osição Comum do Conselho.* [Em linha] Disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:343:0054:0056:PT:PDF [Consult. 14 janeiro 2012]

Conselho da União Europeia, 2001b. *Convenção sobre o Cibercrime.* [Em linha] Disponível em: http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_Portugese.pdf [Consult. 29 novembro 2011]

Conselho de Ministros, 2003. *Conceito Estratégico de Defesa Nacional* (Resolução de Conselho de Ministros nº6/03 de 20 de janeiro), Lisboa: Diário da República

Conselho de Ministros, 2012. *Aprova o plano global estratégico de racionalização e redução de custos com as TIC na Administração Pública* (Resolução do Conselho de Ministros n.º 12/2012 de 07 de fevereiro), Lisboa: Diário da República

Couto, AC, 1988. *Elementos de Estratégia: Apontamentos para um curso Vol I.* Lisboa: IAEM

Denning, D, 2000. *Cyberterrorism.* [Em linha] Disponível em: http://www.cs.georgetown.edu/~denning/publications.html[Consult. 29 dezembro 2011]

Dias, VC, 2011. *De Terrorismo Convencional ao Ciberterrorismo: Um Estudo de Caso Sobre o Papel da AL-QAEDA.* [Em linha] Disponível em: http://macua.blogs.com/files/do-terrorismo-convencional-ao-ciberterrorismo-al-qaeda.pdf [Consult. 31 outubro 2011]

Dougherty, J et al., 2003. *Relações Internacionais: As Teorias em Confronto.* 1ª ed. Lisboa: Gradiva

ENISA, 2012. *About ENISA.* [Em linha] Disponível em: http://www.enisa.europa.eu/ [Consult. 13 fevereiro 2012]

Exército Português, 2007. *PDE 5-00: Planeamento Táctico e Tomada de Decisão.* Lisboa: Exército

FCCN, 2011. *Anunciados resultados de fórum para a cibersegurança.* [Em linha] Disponível em: http://www.cert.pt/index.php/pt/noticias/1612-anunciados-resultados-de-forum-para-a-ciberseguranca [Consult. 18 janeiro 2012]

FCCN, 2012. *Resposta a Incidentes de Segurança "CERT.PT".* [Em linha] Disponível em: http://www.fccn.pt/pt/servicos/seguranca/resposta-a-incidentes-de-seguranca-cert-pt/ [Consult. 18 janeiro 2012]

Federal Ministry of the Interior, 2011. *Cyber Security Strategy for Germany.* Berlin: Department IT 3

Ferreira, L, 2008. Comunicações e Segurança. *Plaenamento Civil de Emergência,* nº20, pp. 42-45

Geers, K, 2011. *Strategic Cyber Security.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence

Gouveia, LB et al., 2004. S*istemas de Informação de Apoio à Gestão.* Porto: SPI – Sociedade Portuguesa de Inovação

GPTIC, 2011. *Plano global estratégico de racionalização e redução de custos nas TIC, na Administração Pública,* Lisboa: s.n.

Graça, PB, 2009. *Mundo Secreto: História do Presente e Intelligence nas Relações Internacionais.* Lisboa: UTL - ISCSP

Guedes, AM, 2007. *Ligações Perigosas.* Coimbra: Almedina

Guedes, AM, 2012. *Terrorismo: A Interrupção de Sistemas.* Entrevistado por Alexandre Varino. Lisboa, 26 janeiro 2012

Hawks, BB, s.d. *Cyber Terror : The Borderless Danger*. [Em linha] Disponível em: http://www.inter-disciplinary.net/wp-content/uploads/2011/05/banuhawksepaper.pdf [Consult. 29 dezembro 2011]

Hughes, RB, 2009. *NATO and Cyber Defence.* [Em linha] Disponível em: http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.Pdf [Consult. 13 fevereiro 2012]

INE, 2012. *Conceitos.* [Em linha] Disponível em: http://metaweb.ine.pt/sim/conceitos/conceitos.aspx?ID=PT [Consult. 7 janeiro 2012]

INTERPOL, 2011. *Cybercrime.* [Em linha] Disponível em: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime [Consult. 29 dezembro 2011]

Jarmon, J, 2011. Cyber-terrorism. *Journal on Terrorism and Security Analysis*, Primavera, pp. 102-117

Jenkins, BM, s.d. *The New Age of Terrorism.* [Em linha] Disponível em: http://www.rand.org/pubs/reprints/2006/RAND_RP1215.pdf [Consult. 14 janeiro 2012]

Jr., JN, 2002. *Compreender os Conflitos Internacionais: Uma Introdução à Teoria e à História.* 3ª ed. Lisboa: Gradiva

Laudon, K et al., 2002. *Management Information Systems.* 7ª ed. New Jersey: Prentice Hall

Leandro, G, 2004. Uma visão militar sobre o terrorismo. In: *Terrorismo.* Coimbra: Almedina

Lord, KM et al., 2011. *America's Cyber Future: Security and Prosperity in the Information Age, Vol I.* Washington: Center for a New American Security

Mascarenhas, AM, 2012. *Planeamento Estratégico.* IESM, 8 fevereiro 2012. Lisboa

Mathias, L, 2009. A Diplomacia como instrumento na luta contra o terrorismo. In: IESM, ed. *Terrorismo Transnacional: Estratégias de Prevenção e de Resposta.* Lisboa: Tipografia Lousanense, p. 132

McConnell, M, 2011. Cyber insecurities:The 21st Century Threatscape. In: *America's Cyber Future: Security and Prosperity in the Information Age, Vol II.* Washington: Center for a New American Security, pp. 27-39

Meireles, M, 2001. *Sistemas Administrativos Clicentristas.* São Paulo: Arte & Ciência

Mendoza, LME et al., 2006. *European Response to Terrorism: The Cases of Spain and Slovakia.* Bratislava: Dalibor Pavolka

Moreira, A et al., 2004. *Terrorismo.* Coimbra: Almedina

NATO, 2009. *AAP-6 NATO Glossary of Terms and Definitions.* Brussels: NATO

NATO, 2010. *Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation.* [Em linha] Disponível em: http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf [Consult. 14 janeiro 2012]

NATO, 2011. *Defending the networks: The NATO Policy on Cyber Defence.* [Em linha] Disponível em: http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf [Consult. 13 fevereiro 2012]

Nunes, PFV, 2009. Ciberterrorismo: Aspectos de Segurança. *Revista Militar,* 25 junho

Nunes, PFV, 2012. *Terrorismo: A Interrupção de Sistemas.* Entrevistado por Alexandre Varino. EME, Lisboa, 12 janeiro 2012

Pais, I et al., 2007. PROTECÇÃO DE INFRA-ESTRUTURAS CRÍTICAS – A COOPERAÇÃO PÚBLICO-PRIVADA. In: *Riscos Públicos e Industriais.* Lisboa: IST, pp. 65-83

Pais, I et al., 2009. Paradigmas da Protecção de Infra-estruturas Críticas e o Estado da Arte em Portugal. *Planeamento Civil de Emergência,* nº 21, pp. 36-43

Pais, I et al., 2010. O Significado da Transposição para Portugal da Directiva Europeia. *Planeamento Civil de Emergência,* nº22, pp. 30-37

Perles, JB, s.d. *Comunicação: conceitos, fundamentos e história.* [Em linha] Disponível em: http://www.bocc.ubi.pt/pag/perles-joao-comunicacao-conceitos-fundamentos-historia.pdf [Consult. 9 novembro 2011]

PORDATA, 2011. *Agregados domésticos privados com computador, com ligação à Internet e com ligação à Internet através de banda larga (%) em Portugal.* [Em linha] Disponível em: http://www.pordata.pt/Portugal/Agregados+domesticos+privados+com+computador++com+ligacao+a+Internet+e+com+ligacao+a+Internet+atraves+de+banda+larga+(percentagem)-1158 [Consult. 5 janeiro 2012]

Quivy, R et al., 2008. *Manual de Investigação em Ciências Sociais.* Lisboa: Gradiva

Roberts, A, 2002. *The Changing Faces of Terrorism.* [Em linha] Disponível em: http://www.bbc.co.uk/history/recent/sept_11/changing_faces_01.shtml [Consult. 9 janeiro 2012]

Rocha, MT, 2007-2008. Protecção de Infra-estruturas Críticas. *Segurança e Defesa,* dezembro-fevereiro, pp. 133-143

Rogeiro, N, 2004. O novo terrorismo internacional como desafio emergente de segurança: Novas e velhas dimensões de um conceito problemático. In: A. Moreira, ed. *Terrorismo.* Coimbra: Almedina, pp. 479-501

Santos, JALd, 2003. *A Idade Imperial: A Nova Era.* 2 ª ed. Mem Martins: Publicações Europa-América

Santos, JALd, 2009. Responder ao Terrorismo - cooperação inter-departamental na luta contra o Terrorismo: opções para uma estrutura integrada de resposta ao Terrorismo e outras Criminalidades Transnacionais. In: IESM, ed. *Terrorismo Transnacional: Estratégias de Prevenção e de Resposta.* Lisboa: Tipografia Lousanense, p. 164

Santos, L, 2008. Terrorismo e Ciberespaço. *Planeamento Civil de Emergência,* nº20, pp. 26-31

Santos, L, 2012. *A Interrupção de Sistemas.* Entrevistado por Alexandre Varino. FCCN, Lisboa, 02 mar 2012

Silva, JMAd, 2009. Desenvolvimento e Terrorismo. In: IESM, ed. *Terrorismo Transnacional: Estratégias de Prevenção e de Resposta.* Lisboa: Tipografia Lousanense, p. 139

Tavares, A e Pais, I, 2012. *A Interrupção de Sistemas.* Entrevistados por Alexandre Varino. CNPCE, Lisboa, 17 fev 2012

Teixeira, NS, 2009. Instrumentos policiais de combate ao Terrorismo. A articulação dos sistemas de preparação e de resposta a emergências. In: IESM, ed. *Terrorismo Transnacional: Estratégias de Prevenção de de Resposta.* Lisboa: Tipografia Lousanense, p. 156

Thornton, HL, 2010. *Countering Radicalism with a "Virtual Library of Freedom".* [Em linha] Disponível em: http://irtheoryandpractice.wm.edu/projects/PIPS/0910/Thornton.PB.pdf [Consult. 29 dezembro 2011]

Tikk, E, 2011. *Frameworks for International Cyber Security: National Cyber Security Policies and Strategies.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence

União Europeia, 2003. *Estratégia Europeia em Matéria de Segurança.* [Em linha] Disponível em: http://consilium.europa.eu/uedocs/cmsUpload/031208ESSIIP.pdf [Consult. 17 janeiro 2012]

União Europeia, 2005. *Livro Verde relativo a um Programa Europeu de Proteção das Infraestruturas Críticas.* [Em linha] Disponível em: http://eur-lex.europa.eu/LexUriServ/site/pt/com/2005/com2005_0576pt01.pdf [Consult. 3 fevereiro 2012]

União Europeia, 2010. *Programa Europeu de Protecção das Infra-Estruturas Críticas.* [Em linha] Disponível em: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_pt.htm [Consult. 30 janeiro 2012]

United Nations, 2001. *Resolution 1373.* [Em linha] Disponível em: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement
[Consult. 14 janeiro 2012]

United States Army Training and Doctrine Command, 2007. *Military Guide to Terrorism in the Twenty-First Century.* Kansas: TRADOC G2

United States Departement of State, 2011. *Foreign Terrorist Organizations.* [Em linha]
Disponível em: http://www.state.gov/s/ct/rls/other/des/123085.htm
[Consult. 3 janeiro 2011]

United States Joint Forces Command, 2010. *JP 3-07.2 - Antiterrorism.* Washington DC: s.n.

Waters, M, 1999. *Globalização.* Oeiras: Celta Editora

Worldometers, 2012. *Worldometers Real Time World Statistics.* [Em linha]
Disponível em: http://www.worldometers.info/ [Consult. 8 janeiro 2012]

Zalman, A, s.d. *The History of Terrorism.* [Em linha] Disponível em: http://terrorism.about.com/od/whatisterroris1/p/Terrorism.htm [Consult. 9 janeiro 2012]

Apêndices

Apêndice 1 - Corpo de conceitos

AMEAÇA – É qualquer acontecimento ou ação (em curso ou previsível) que contraria a consecução de um objetivo e que, normalmente é causador de danos, materiais ou morais. Uma ameaça é o produto de uma possibilidade por uma intenção. (Couto, 1988, p. 329).

ANTITERRORISMO – Todas as medidas preventivas e defensivas tomadas no sentido de reduzir as vulnerabilidades de indivíduos, forças e propriedades contra ameaças terroristas (NATO, 2009).

CIBERATAQUE - É um ataque efetuado no ciberespaço, dirigido contra um ou vários sistemas de informação e destinado a prejudicar a sua segurança (Federal Ministry of the Interior, 2011).

CIBERCRIME - Ato praticado contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a sua utilização fraudulenta (Conselho da União Europeia, 2001b).

CIBERESPAÇO – É um domínio caracterizado pelo uso da eletrónica e do espectro eletromagnético para armazenar, modificar e trocar dados através de sistemas em rede e das infraestruturas físicas associadas. Fisicamente, é o *hardware*, o *software*, e os elementos de transporte que equivalem às arquiteturas de rede por meio do qual a energia passa, fornecendo informações (Jarmon, 2011).

CIBERESPIONAGEM - São ciberataques dirigidos contra a confidencialidade de um sistema de informação, que são efetuados e geridos por serviços de informação estrangeiros (Federal Ministry of the Interior, 2011).

CIBERGUERRA - Consiste nas operações militares conduzidas no ciberespaço para negar a um adversário, estatal ou não-estatal, o uso efetivo dos sistemas de informação, de armas, ou os sistemas controlados por tecnologias de informação, a fim de alcançar um fim político (Lord et al., 2011).

CIBERSABOTAGEM - São ciberataques dirigidos contra a integridade e disponibilidade dos sistemas de informação (Federal Ministry of the Interior, 2011).

CIBERSEGURANÇA – É a proteção dos computadores, da informação eletrónica ou redes digitais, contra a divulgação não autorizada, a transferência, a negação, a modificação ou destruição, acidental ou intencional (Lord et al., 2011).

CIBERTERRORISMO - São ataques ilegais ou ameaças de ataques contra os computadores, redes e as informações neles armazenadas, efetuados para intimidar ou coagir um Governo ou o seu povo em prol de objetivos políticos ou sociais (Denning, 2000).

CONTRATERRORISMO – Todas as medidas ofensivas tomadas para neutralizar o terrorismo, antes ou depois de atos hostis terem ocorrido (NATO, 2009).

ESTRATÉGIA – É a ciência e a arte de desenvolver e utilizar as forças morais e materiais de uma unidade política ou coligação, a fim de se atingirem objetivos políticos que suscitam, ou podem suscitar, a hostilidade de uma outra vontade política (Couto, 1988).

HACKING - São atividades realizadas *on-line* e de forma encoberta, que procuram revelar, manipular ou explorar vulnerabilidades nos sistemas operativos dos computador e outros *softwares* (Hawks, s.d.).

HACKTIVISMO - Uso ilegal ou de legalidade duvidosa, mas não violenta, de ferramentas digitais com objetivos políticos (Hawks, s.d.).

INFORMAÇÃO – É uma coleção de dados que, quando apresentada de determinada forma e em determinado momento, melhora o conhecimento do indivíduo que a recebe, de modo a que este indivíduo se torne mais capaz de realizar a ação ou decisão a que se propõe (Galliers, 1987 cit. por Gouveia et al., 2004, p. 10).

INFRAESTRUTURA CRÍTICA - A componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções (Assembleia da República, 2011).

INFRAESTRUTURA CRÍTICA EUROPEIA - É a infraestrutura crítica situada em território nacional cuja perturbação ou destruição teria um impacto significativo em, pelo menos, mais um Estado membro da União Europeia, sendo o impacto avaliado em função de critérios transversais, incluindo os efeitos resultantes de dependências intersectoriais em relação a outros tipos de infra -estruturas (Assembleia da República, 2011).

SISTEMA - Conjunto de partes interdependentes que, juntas, formam um todo unitário (Meireles, 2001).

RISCO - É a possibilidade de perigo ou acontecimento indesejado. É caracterizado pelo grau de probabilidade e de severidade de uma potencial perda resultante de perigos devido à presença de um inimigo ou outras condições adversas. O nível de risco é expresso em termos de probabilidade e severidade de perigo (Exército Português, 2007).

SISTEMA INFORMÁTICO – Qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados,

tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção (Assembleia da República, 2009c).

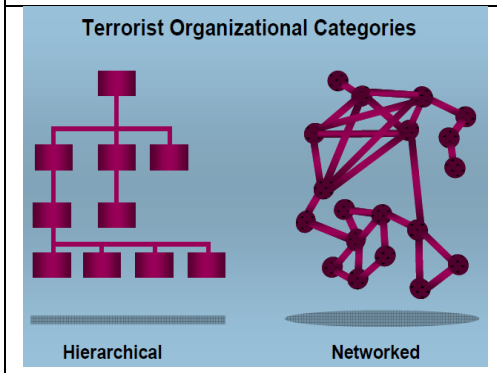
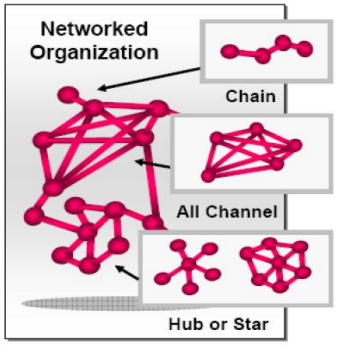
SISTEMAS DE INFORMAÇÃO – Somatório de componentes interligados que trabalham em conjunto para recolher, processar, armazenar e disseminar informação para apoio à tomada de decisão, coordenação, controlo, análise e visualização dessa informação numa organização (Laudon et al., 2002).

TECNOLOGIAS DE INFORMAÇÃO - Engloba os dispositivos de computador (*hardware* e *software*), tecnologias de dados de armazenamento, técnicas de processamento e tecnologias de comunicação de dados e de informação (Gouveia et al., 2004, p. 22).

TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO - Adiciona às tecnologias de informação, as preocupações com a comunicação de informação, nomeadamente as questões de mediação de base digital entre indivíduos, suporte a grupos, apresentação e visualização de dados e informação (Gouveia et al., 2004, p. 22).

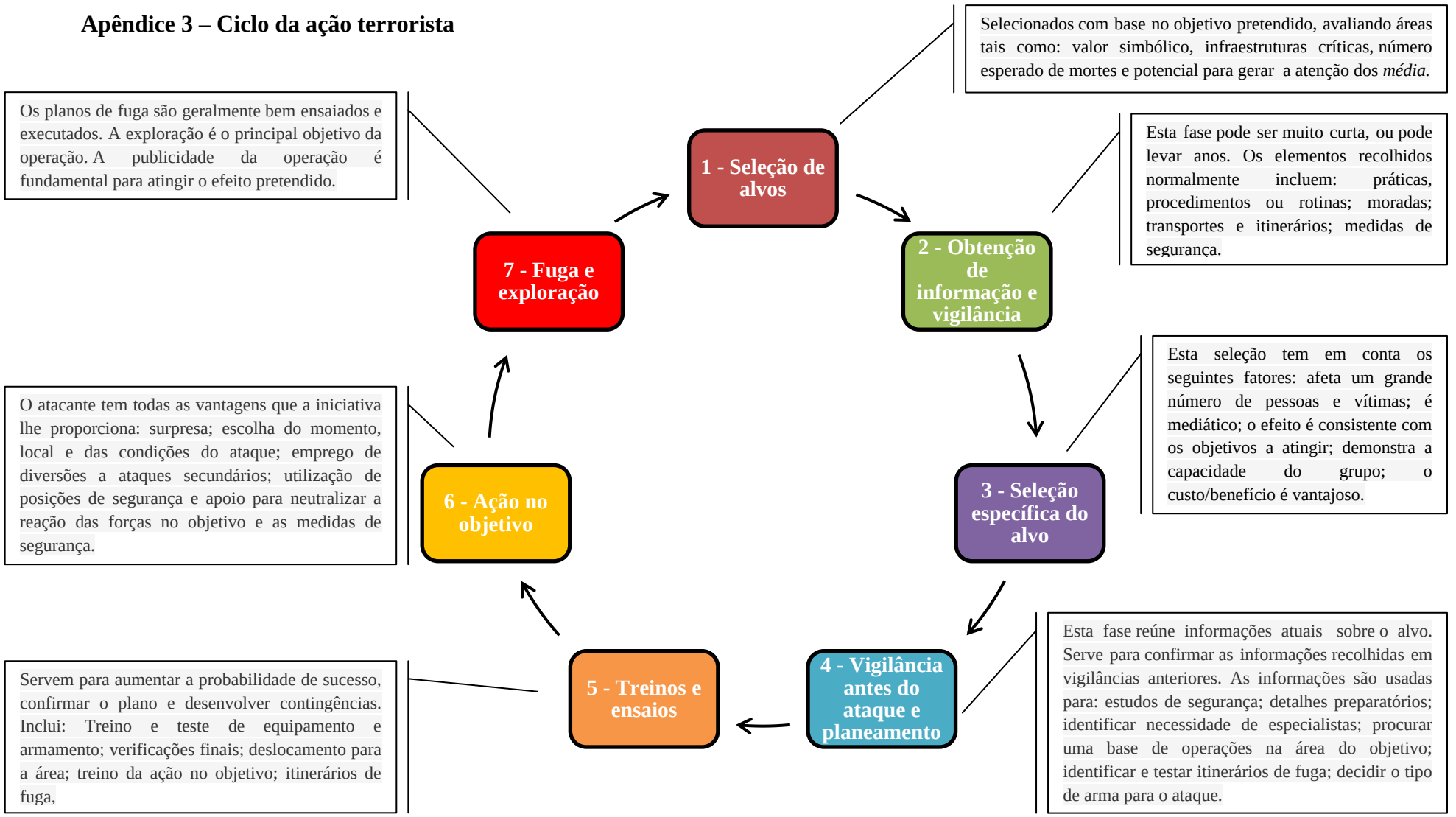
TERRORISMO – O uso ilegal da força ou da violência ou a ameaça de uso contra pessoas ou propriedades, na tentativa de coagir ou intimidar Governos ou sociedades para alcançar objetivos políticos, religiosos ou ideológicos (NATO, 2009). Designa um sistema, ou regime, baseado no medo provocado por atos de violência calculada, geralmente indiscriminada, de cariz eminentemente político, que não se confunde com a delinquência comum (Rogeiro, 2004, p. 481).

Apêndice 2 – Formas de organização, recrutamento e financiamento das organizações terroristas

<table>
<tr><th colspan="2">ORGANIZAÇÃO</th><th>RECRUTAMENTO</th><th>FINANCIAMENTO</th></tr>
<tr><th>HIERÁRQUICA</th><th>REDE</th><td rowspan="3">É normalmente efetuado junto das populações que são simpatizantes das ideologias e dos objetivos dos grupos terroristas. Muitas vezes, organizações legítimas podem servir como fonte de recrutamento de terroristas. Por exemplo, o recrutamento de militantes islâmicos tem sido associada às escolas (madraças), dirigidas por clérigos radicais islâmicos.
Alguns recrutamentos são feitos com base em competências e qualificações (pessoal com experiência NBQR, informáticos, militares). O recrutamento é frequentemente dirigido a grupos alvo que se sentem marginalizados, tais como prisioneiros, desempregados, pobres e imigrantes.
Outra forma de recrutamento é através da coerção. Esta, pode variar desde a obtenção de informações até à realização de atentados suicidas. A chantagem e intimidação são as formas mais comuns de coerção.
Os modernos sistemas de informação, são amplamente utilizados para a difusão de propaganda e como meios de recrutamento.</td><td rowspan="3">Os grupos terroristas desenvolveram várias formas de financiamento, das quais se destacam: apoio estatal; financiamento proveniente de resgates; extorsão e esquemas de proteção; fraudes de vários tipos, incluindo a informática; investimentos, muitos deles legais; tráfico de drogas, armamento e de seres humanos; contribuições privadas, de diásporas étnicas, comunidades de emigrantes e simpatizantes, especialmente quando as organizações estão de alguma forma ligadas à religião.</td></tr>
<tr><td>Cadeia de Comando vertical e bem definida. A informação flui verticalmente. É uma organização comum de grupos bem estabelecidos com uma estrutura de comando e de apoio. Apresentam uma maior especialização de funções nas suas células subordinadas (apoio, operações, informações).
Têm um conjunto claramente definido de objetivos políticos, sociais ou económicos.
A vantagem deste tipo de organização é uma maior eficiência devido à especialização e à capacidade de coordenacão das ações.</td><td>Existe uma distribuição de autoridade e de responsabilidade em toda a organização, criando frequentemente funções chave redundantes. Para ser eficaz, esta organização necessita de uma ideia, objetivo ou ideologia unificadora. Os objetivos gerais e as metas a atingir são anunciados, e os indivíduos ou células pertencentes à organização devem usar a flexibilidade e a iniciativa para realizar as ações necessárias para atingir esses objetivos.
Existem três tipos básicos de organização em rede:
- em cadeia ou linha;
- radial ou estrela;
- em todos os sentidos.</td></tr>
<tr><td> 
</td><td> 
</td></tr>
</table>

Fontes: JP 3-07.2 - Antiterrorism (2010); A Military Guide to Terrorism in the Twenty-First Century (2007); The New Age of Terrorism

Apêndice 3 – Ciclo da ação terrorista



Fonte: A Military Guide to Terrorism in the Twenty-First Century (2007)

Apêndice 4 - As ciberameaças do século XXI

ATORES	Estados	Representam a ameaça mais poderosa e significativa do ciberespaço. Estas ameaças vão desde desinformação a ataques de pequena e grande escala sobre infraestruturas críticas.
	Organizações não estatais	Organizações ideológicas ou criminosas podem conduzir ataques cibernéticos para negar ou perturbar o serviço de sistemas, mas não têm as mesmas capacidades que os Governos.
	Indivíduos	São potenciais adversários cibernéticos, que se dividem em quatro grupos principais: os novatos, *hackers*, hackerativistas e terroristas cibernéticos.
VETORES	Cinéticos	São ataques em que se utiliza a força física, tal como um engenho explosivo, um míssil, uma bomba ou mesmo um objeto contundente, para infligir danos graves ou destruir um alvo que representa um nó ou um componente crítico de uma rede de informações, de comunicações ou de comando de um Estado ou organização.
	Eletromagnéticos	Podem ser gerados Impulsos eletromagnéticos de grande potência, capazes de interferir com os sistemas elétricos e paralisar as redes elétricas de uma região. Estes impulsos podem também destruir fisicamente componentes chave dos computadores, como por exemplo a motherboard.
	Cibernéticos	A maioria das ciberameaças são não-cinéticas, são os programas de *software* malicioso e ataques DoS (*Denial-of-Service*)
ALVOS	Estatais	São sobretudo as Infraestruturas críticas, cuja destruição total ou parcial, disfunção ou utilização indevida pode afetar, direta ou indiretamente, de forma permanente ou prolongado o seu funcionamento.
	Civis	
	Militares	

Fonte: McConnell (2011)

Apêndice 5 - Lista dos principais ciberataques desde 2002

ANO	CIBERATAQUE
2002	O apoio financeiro dos atentados de 2002 em Bali, foram obtidos através de fraudes *on-line* de cartões de crédito.
2003	Uma operação de *hacking* na Rússia, de fraude e extorsão, originou perdas de cerca de 25 milhões dólares.
2004	Uma investigação nos EUA, que ficou conhecida como "Operação Firewall ", pôs fim a uma organização criminosa que envolvia 4.000 membros envolvidos no roubo de identidades e informações de cartões de crédito.
2005	Um jovem de Massachusetts foi responsável pelo roubo de informações pessoais e por criar o pânico com ameaças de bomba (o jovem invadiu a internet e prestadores de serviços telefónicos durante um período de 15 meses antes ser preso).
maio 2006	As redes dos Departamentos de Estado dos EUA foram atacadas por *hackers* estrangeiros, e foram feitos *downloads* de *terabytes* de informação.
agosto 2006	Um oficial sénior da Força Aérea Americana declarou publicamente que, a China tinha feito o *download* de 10 a 20 *terabytes* de dados da NIPRNet (a rede militar não classificada).
maio 2007	A Estónia sofreu um ataque, presumivelmente a partir da Rússia, que paralisou por completo o país durante semanas.
agosto 2007	Os serviços de segurança britânicos, o gabinete do primeiro-ministro francês, e o gabinete da chanceler alemã Merkel, queixaram-se de que teriam sido alvo de intrusões eletrônicas por parte da República Popular da China.
setembro 2007	Israel interrompeu as redes de defesa aérea Sírias, durante o bombardeamento de uma alegada instalação nuclear síria .
outubro 2007	O Ministro da Segurança chinês afirmou que hackers estrangeiros, 42% a partir de Taiwan e 25% dos EUA, tinham roubado informações de áreas chave chinesas.
março 2008	Funcionários sul-coreanos referiram que a China tinha tentado invadir a embaixada da Coreia e as suas redes militares.
agosto 2008	As redes de computadores na Geórgia foram invadidas por intrusos estrangeiros desconhecidos, presumivelmente a mando do governam russo.
novembro 2008	*Hackers* violaram as redes do *Royal Bank of Scotland*, clonaram 100 cartões ATM e retiraram mais de 9 milhões de dólares a partir de máquinas de 49 cidades.
novembro 2008	As redes classificadas do Departamento de Defesa dos EUA foram invadidas por invasores desconhecidos estrangeiros, tendo levado vários dias para os remover e recuperar as redes.
janeiro 2009	*Hackers* atacaram a infraestrutura de internet de Israel durante a ofensiva militar na Faixa de Gaza. O ataque, que se concentrou em *sites* do Governo, foi executado por pelo menos cinco milhões de computadores. As autoridades israelitas acreditam que o ataque foi realizado por uma organização criminosa da antiga União Soviética, e pago pelo Hamas ou pelo Hezbollah.
fevereiro 2009	600 computadores do Ministério dos Negócios Estrangeiros da India foram atacados.
julho 2009	Foram lançados ciberataques contra *sites* nos EUA e na Coreia do Sul, incluindo sites do Governo, por *hackers* desconhecidos. A Coreia do Sul acusou a Coreia do Norte de estar por detrás dos ataques. Apesar da negação de serviço não causar graves perturbações, o facto de ter durado vários dias, gerou uma grande atenção da comunicação social.
dezembro 2009	Insurgentes iraquianos tiveram acesso às imagens transmitidas pelos UAVs americanos.
janeiro 2010	A Google anunciou que um ataque tinha penetrado as suas redes, juntamente com as redes de mais de 30 outras empresas dos EUA.

março 2010	A NATO e a UE alertaram que o número de ataques cibernéticos contra as suas redes tinham aumentado significativamente nos últimos 12 meses e que a Rússia e China estavam entre os adversários mais ativos.
abril 2010	*Hackers* chineses supostamente invadiram arquivos classificados do Ministério da Defesa indiano e de embaixadas indianas em todo o mundo, obtendo acesso a sistemas de armamento e a mísseis indianos.
outubro 2010	O Diretor das Comunicações de Defesa da Austrália relatou um enorme aumento em ciberataques sobre os sistemas militares, tendo o próprio Ministro da Defesa revelado que houve 2.400 incidentes de segurança eletrónica nas redes de defesa em 2009 e 5551 incidentes entre janeiro e agosto de 2010.
janeiro 2011	O Governo canadiano relatou um ataque cibernético contra suas principais agências, incluindo a de Pesquisa e Desenvolvimento de Defesa. O ataque forçou o departamento de Finanças e de Tesouraria, bem como as principais agências económicas a desligar-se da internet. Fontes canadianas atribuem o ataque à China.
março 2011	*Hackers* penetraram nas redes de computadores do Governo francês, procurando informações sobre os próximos encontros do G-20.
junho 2011	O Citibank informou que os dados dos cartões de crédito de 360 mil clientes foram roubados.
setembro 2011	O Diretor das Comunicações de Defesa da Austrália relatou que as redes de defesa são atacadas mais de 30 vezes por dia e que o número de ataques aumentou em mais de 350% comparativamente com 2009.
novembro 2011	*Hackers* atacaram os *sites* do Parlamento português, dos partidos políticos, do Ministério da Administração Interna, divulgando dados pessoais de polícias, bem como o portal das finanças e o site do Hospital da Cruz Vermelha.

Fonte: Jack Jarmon (2011); Center for Strategic and International Studies (EUA – 2006); Jornal Público (30-11-2011)

Apêndice 6 – A estrutura portuguesa de prevenção e combate ao terrorismo

As Organizações Internacionais (OI) das quais Portugal faz parte condenam e elegem o terrorismo, como uma das principais ameaças para a segurança dos seus membros. Para a Organização das Nações Unidas (ONU) (2001), o terrorismo internacional constitui uma das mais sérias ameaças à paz e segurança internacional no século XXI. É uma ameaça condenável, que deve ser prevenida e combatida por todos os meios, cuja atuação, financiamento e apoio deverá ser punido por lei e cujo direito de defesa individual e coletiva é reconhecido pela sua Carta. Também a NATO (2010), em completa sintonia com a ONU, refere no seu Conceito Estratégico[20], que o terrorismo constitui uma ameaça direta à segurança, à estabilidade internacional e à prosperidade dos seus membros. A União Europeia declarou que o terrorismo constitui um verdadeiro desafio e que o seu combate passaria a ser um objetivo prioritário (Conselho da União Europeia, 2001a), pois este põe vidas em risco, implica custos avultados, procura abalar a abertura e a tolerância das sociedades europeias e representa uma crescente ameaça estratégica para toda a Europa (União Europeia, 2003).

Perante a assunção de que o terrorismo constitui de facto uma ameaça real, Portugal tomou medidas no sentido de a prevenir e combater, legislando[21] a punição dos atos e das organizações terroristas, organizando tanto as Forças e Serviços de Segurança, como as FFAA de forma a poder combatê-la.

Segundo o Sr. Gen Loureiro dos Santos (2009, pp. 165-167), na luta contra o terrorismo poderão ser empregues quatro formas de atuação estratégica. Podem-se-lhes retirar os apoios, diminuir e se possível terminar o universo de recrutamento, dar-lhes luta efetiva, e organizar o emprego de uma estrutura, meios e procedimentos de socorro e emergência em caso de atentado. Iremos de seguida determo-nos sobre as competências das Forças e Serviços de Segurança e das FFAA, na prevenção e luta contra esta ameaça.

(1) O papel das Forças e Serviços de Segurança

A segurança interna é a atividade desenvolvida pelo Estado para garantir a ordem, a segurança e a tranquilidade públicas, proteger pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o normal funcionamento das instituições

[20] Assinado em Lisboa em 2010.
[21] Lei nº 52/2003 de 22 de Agosto (Assembleia da república, 2003).

democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática, designadamente contra o terrorismo[22].

Exercem funções de segurança interna a Guarda Nacional Republicana (GNR), a Polícia de Segurança Pública (PSP), a Polícia Judiciária (PJ), o Serviço de Estrangeiros e Fronteiras (SEF) e o Serviço de Informações de Segurança (SIS)[23].

No âmbito do combate ao terrorismo, compete à Unidade de Coordenação Antiterrorismo[24] garantir a coordenação e a partilha de informação, entre os serviços que a integram[25]. O SIS é o único organismo incumbido da produção de informações destinadas a garantir a segurança interna e necessárias a prevenir o terrorismo[26], sendo da PJ a competência reservada da investigação dos crimes de organizações terroristas e terrorismo[27], que para isso tem a Unidade Nacional Contra Terrorismo[28].

As FFAA colaboram em matéria de segurança interna nos termos da Constituição e da lei, competindo ao Secretário-geral do Sistema de Segurança Interna e ao Chefe do Estado Maior General das Forças Armadas (CEMGFA) assegurarem entre si a articulação operacional[29]. A natureza transnacional do terrorismo levará ao esbatimento das divisões e ao necessário e benéfico aumento da cooperação e complementaridade das FFAA e das Forças de Segurança no seu combate. Situação que de igual modo deverá acontecer no "instrumento fulcral" de prevenção e combate que são os serviços de informações (Teixeira, 2009, p. 158).

(2) O papel das Forças Armadas

De acordo com o Conceito Estratégico de Defesa Nacional, o "terrorismo transnacional assume uma possibilidade de atuação à escala global, conjugando a violência tradicional, decorrente de atentados e ações bombistas, com a possível utilização do ciberespaço e de meios de destruição massiva. As consequências de tais ações nas

[22] Artigo 1º da Lei nº 53/2008 – Lei de Segurança Interna (Assembleia da república, 2008c).
[23] Artigo 25º da Lei nº 53/2008 – Lei de Segurança Interna (Assembleia da república, 2008c).
[24] Constituída por: os Secretários Gerais do Sistema de Segurança Interna e do Sistema de Informações da República Portuguesa; o Comandante Geral da Guarda Nacional Republicana, os Diretores Nacionais da Polícia de Segurança Pública, da Polícia Judiciária e do Serviço de Estrangeiros e Fronteiras e os Diretores do Serviço de Informações Estratégicas de Defesa e do Serviço de Informações de Segurança; a Autoridade Marítima Nacional.
[25] Artigo 23º da Lei nº 53/2008 – Lei de Segurança Interna (Assembleia da república, 2008c).
[26] Artigo 3º da Lei nº 9/2007 – Lei Orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa (SIED) e do Serviço de Informações de Segurança (SIS) (Assembleia da república, 2007).
[27] Artigo 7º da Lei nº 49/2008 – Lei de Organização da Investigação Criminal (Assembleia da república, 2008b).
[28] Artigo 28º da Lei nº 37/2008 – Lei Orgânica da Polícia Judiciária (Assembleia da república, 2008a).
[29] Artigo 35º da Lei nº 53/2008 – Lei de Segurança Interna (Assembleia da república, 2008c).

economias, na segurança e na estabilidade internacionais transcendem a capacidade de resposta individualizada dos Estados e interrelacionam os conceitos de segurança interna e externa e os objetivos que estes prefiguram. O terrorismo transnacional apresenta-se, pois, como uma ameaça externa e, quando concretizado, como uma agressão externa, pelo que a sua prevenção e combate se inserem claramente na missão das FFAA. Para o cumprimento desta missão, as FFAA deverão ter capacidade para, em colaboração com as forças de segurança, na ordem interna, e em estreita relação com os aliados, na ordem externa, prevenir e fazer face às ameaças terroristas" (Conselho de Ministros, 2003). Esta mesma missão vem plasmada no Artigo 4º da Lei Orgânica de Bases da Organização das Forças Armadas (LOBOFA), onde refere, que estas deverão "cooperar com as forças e serviços de segurança tendo em vista o cumprimento conjugado das respetivas missões no combate a agressões ou ameaças transnacionais" (Assembleia da República, 2009a).

Não sendo a prevenção de ações terroristas da responsabilidade principal das FFAA, estas, deverão possuir, no entanto, a capacidade de participar na segurança interna e estar prontas a fazê-lo. "Esta intervenção poderá ser feita em articulação com outras forças de natureza policial, reforçando-as na defesa de pontos e áreas sensíveis que possam ser objeto de ataques terroristas (aeroportos, espaço aéreo, instalações portuárias, grandes e vulneráveis infraestruturas de transportes terrestres, centros de comunicações, centrais produtoras de energia e de distribuição de água, edifícios governamentais e simbólicos, etc.), utilização dos serviços de informações militares, dos meios militares de comando e controlo e de efetivos de combate". Em aditamento a esta prevenção interna, a intervenção das FFAA também no exterior do país, atuando no âmbito das organizações a que Portugal faz parte, ajudando na estabilização e recuperação de países instáveis, desorganizados e anárquicos, e impedindo que estes se constituam como santuários para redes terroristas, é uma outra forma de prevenção e combate (Santos, 2003, pp. 225-227).

Anexos

Anexo A - Sectores estratégicos a que pertencem as infraestruturas críticas

1. Sistematização da UE

SECTOR	PRODUTO OU SERVIÇO
I - Energia	• Produção de petróleo e gás, refinamento, tratamento e armazenamento incluindo *pipelines.* • Geração de Eletricidade • Transmissão e distribuição de Eletricidade, Gás e Petróleo.
II - Tecnologias de Informação e Comunicação	• Sistemas de Informação e Proteção de Redes de Telecomunicações. • Instrumentos De Automatização e de Controlo de Sistemas (SCADA, etc). • Internet • Fornecimento de redes de telecomunicações fixas • Fornecimento de redes de telecomunicações móveis • Comunicação e navegação por Radio • Comunicação por Satélite • *Broadcasting* – distribuição de sinais de áudio e radio
III - Água	• Sistemas de distribuição de água potável • Sistemas de controlo da qualidade da água • Sistemas de controlo da quantidade e caudal de água
IV - Alimentação	• Sistemas de aprovisionamento e proteção de alimentos em condições de segurança e qualidade
V - Saúde	• Serviços Médicos e Cuidados Hospitalares • Serviços e Produtos Farmacêuticos – vacinas, medicamentos • Bio-Laboratórios e Bio-Agentes
VI - Financeiro	• Serviços e Estruturas de Pagamentos • Serviços Financeiros dos Governos
VII – Segurança Pública	• Manutenção dos serviços de segurança, integridade e boa ordem pública • Administração da Justiça e Processos de Detenção
VIII – Administração Civil	• Funções de Governação • Forças Armadas • Serviços de Administração Civil • Serviços de Emergência • Serviços de Correios e Entregas Postais
IX - Transportes	• Transportes Rodoviários • Transportes Ferroviários • Transportes Aéreos • Transportes Marítimos internos • Transportes Marítimos em oceanos - longa e curta duração
X – Indústria Química e Nuclear	• Produção e armazenamento/processamento de substâncias químicas e nucleares • *Pipelines* de produtos perigosos (substâncias químicas)
XI – Espaço e Investigação	• Espaço • Investigação

Fonte: Comissão das Comunidades Europeias - Livro verde relativo a um Programa Europeu de Proteção das Infraestruturas Críticas (2005)

2. Sistematização portuguesa

PILAR	SECTOR	SUB-SECTOR
Sustentabilidade	Energia	• Energia elétrica • Combustíveis • Gás natural
	Comunicações	• Comunicações Fixas • Comunicações Móveis • Comunicações de Dados e internet • Serviços postais
	Transportes	• Transportes Aéreos • Transportes Marítimos • Transportes Terrestres • Transportes Fluviais
	Indústria	• Indústria de Alimentação, Bebidas e Tabaco • Indústria da Madeira, Cortiça e Mobiliário • Indústria do Papel • Indústria dos Minerais não metais • Indústria e Comércio automóvel • Indústria Elétrica e Eletrónica • Indústria Extrativa • Indústria Farmacêutica • Indústria Metalúrgica e Metalomecânica • Indústria Química • Indústria Têxtil
	Media	• Radiodifusão • Teledifusão
	Comércio	• Grossista • Retalho
	Serviços Financeiros	• Finanças • Banca
Governação	Órgãos de Soberania	• Presidente da República • Assembleia da República • Governo • Tribunais
	Ministérios	• Ministérios
Segurança	Segurança	• Forças de Segurança • Serviços de Informação • Polícia Judiciária
	Defesa	• Defesa • Exército • Marinha • Força Aérea
	Proteção Civil	• Proteção Civil
Valores Básicos	Água	• Água para rega • Água para consumo humano
	Alimentação	• Áreas alimentares
	Saúde	• Hospitais • Assistência Pré-Hospitalar • Medicamentos • Sangue
	Ambiente	• Ambiente

Fonte: Conselho Nacional de Planeamento Civil de Emergência (2012)